UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

DERECHO PENAL INFORMÁTICO: DESLEGITIMACIÓN DEL PODER PUNITIVO EN LA SOCIEDAD DE CONTROL

TESIS

PRESENTADA POR:

MICHAEL ESPINOZA COILA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

PUNO – PERÚ

2 017

UNIVERSIDAD NACIONAL DEL ALTIPLANO
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS
ESCUELA PROFESIONAL DE DERECHO

DERECHO PENAL INFORMÁTICO: DESLEGITIMACIÓN DEL PODER PUNITIVO EN LA SOCIEDAD DE CONTROL

TESIS PRESENTADA POR:

MICHAEL ESPINOZA COILA

PARA OPTAR EL TITULO PROFESIONAL DE:

ABOGADO

APROBADO POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE:
M. Sc. Jovin Hipólito Valdez Peñaranda

PRIMER MIEMBRO:
Dr. Walter Salvador Gálvez Condori

SEGUNDO MIEMBRO:
M. Sc. Juan Carlos Mendizábal Gallegos

DIRECTOR:
Abog. Reynaldo Luque Mamani

ASESOR:
Prof. Dr. hc. mult. Eugenio Raúl Zaffaroni

Área : Derecho Público
Línea : Derecho Penal
Tema : Teoría General del Delito

FECHA DE SUSTENTACIÓN: 15 DE DICIEMBRE DEL 2 017

DEDICATORIA

Ad:

Deus pater,

parentes Simon et Basilia,

et dilectus meus princeps SCQ.

AGRADECIMIENTO

A mi amigo y maestro en Derecho Penal y Criminología: Dr. Eugenio Raúl Zaffaroni, Profesor Emérito de la Universidad de Buenos Aires y actual integrante de la Corte Interamericana de Derechos Humanos, por su asesoramiento e influencia doctrinaria en este modesto trabajo de investigación.

A los siguientes juristas, por su ayuda bibliográfica: Dr. Matías Bailone (Argentina), Dr. Jan-Michael Simon (Alemania), Dr. Salvador Millaleo Hernández (Chile), Dr. Juan José Gonzáles Rus (España), Dr. Santiago Acurio del Pino (Ecuador), Dr. Gabriel Andrés Cámpoli (México). También al Dr. Jorge Muñiz Ziches, Ex Congresista de la República del Perú.

A los siguientes docentes de la Universidad Nacional del Altiplano de Puno, por sus consejos y motivación: Abog. Reynaldo Luque Mamani, M. Sc. José A. Pineda Gonzales, M. Sc. Juan Casazola Ccama, Dr. Boris G. Espezúa Salmón, M. Sc. Jovin H. Valdez Peñaranda, Dr. Walter S. Gálvez Condori, M. Sc. Juan C. Mendizabal Gallegos, Dr. Javier S. Pineda Ancco y M. Sc. Peregrino Melitón López Paz.

Personal no docente de la Universidad Nacional del Altiplano de Puno, amigos y compañeros universitarios, que me brindaron facilidades para ejecutar la presente investigación.

ÍNDICE GENERAL

IV. RESULTADOS Y DISCUSIÓN

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ACRÓNIMOS

CONS: Constitución Política del Perú (1 993).

CP: Código Penal peruano de 1 991.

TIC: Tecnologías de la Información y la Comunicación.

UNODC: Oficina de Naciones Unidas Contra la Droga y el Delito.

CIA: Agencia Central de Inteligencia.

NSA: Agencia de Seguridad Nacional.

RESUMEN

El trabajo de Tesis obedece a la problemática del poder de vigilancia del poder punitivo habilitado con nuevos delitos asociados a las Tecnologías de la Información y Comunicación (TIC) que emergieron en la legitimada Sociedad de la Información o Sociedad del Riesgo, cuestión que es tratada por el Derecho Informático y el Derecho Penal, sin advertir la pérdida de la privacidad por el incremento de vulnerabilidad de los ciudadanos frente a los agentes ejecutivos, y la selectividad del poder punitivo y la tributación a la Sociedad de Control; nos propusimos como objetivo principal definir el Derecho Penal Informático, y como específicos, explicar sus límites u horizonte de proyección, la interdisciplinariedad del Derecho Informático y el Derecho Penal, sus fuentes, definir el delito informático, describir el tratamiento de los delitos informáticos en el Derecho peruano y comparado, explicar la aplicación espacial y temporal de los delitos informáticos, y señalar las consideraciones de política criminal; la investigación es de Diseño cualitativo-documental; el Universo fue el Derecho Penal y el Derecho Informático, y el objeto de estudio los Delitos Informáticos; los métodos que se utilizaron fueron: El dogmático jurídico, histórico-comparativo, inductivo, deductivo, análisis y síntesis; entre los Resultados más relevantes están la formulación del Derecho Penal Informático Humano, como derivación del Derecho Penal Humano del jurista Eugenio Raúl Zaffaroni, y concluimos de modo general, que el Derecho Penal

Informático Humano, es el saber jurídico penal que mediante la interpretación de leyes penales sobre delitos informáticos, propone a los agentes jurídicos un sistema reductor del poder de vigilancia del poder punitivo en la sociedad de control e impulsar el poder jurídico con el fin de preservar los espacios de libertad y privacidad de las personas; y de modo específico que los límites u horizontes de proyección del Derecho Penal Informático, se explica por su propia definición como saber jurídico, que tiene por objeto estudio la seguridad jurídica, y las leyes penales sobre Delitos Informáticos como objeto de interpretación; tiene la función de reducir el poder de vigilancia del poder punitivo; se caracteriza por ser público, represivo, continuo, fragmentador y normativo; la interdisciplinariedad del Derecho Informático y el Derecho Penal, se explica por su correspondencia de saberes jurídicos de forma secante; asimismo este saber jurídico penal tiene fuentes de conocimiento, de información y de producción (en el caso de leyes penales); sobre la aplicación espacial y temporal, los delitos informáticos son transnacionales, y que se deben emplear los Principios de aplicación temporal del Código Penal; finalmente que la criminalización mediática, ha fomentado los delitos informáticos, y con ella se potencia más el poder punitivo y su poder de vigilancia, y que se puede prevenir los Delitos Informáticos.

Palabras Clave: Delito, informática, sociedad, poder punitivo, control.

ABSTRACT

The work of Thesis obeys to the problematic one of the power of vigilance of the punitive power enabled with new crimes associated to the Technologies of the Information and Communication (TIC) that emerged in the legitimated Society of the Information or Society of the Risk, question that is treated by Computer Law and Criminal Law, without noticing the loss of privacy due to the increased vulnerability of citizens to executive agents, and the selectivity of punitive power and taxation to the Control Society; We proposed as a main objective to define the Criminal Computer Law, and as specific, explain its limits or horizon of projection, the interdisciplinary nature of Computer Law and Criminal Law, its sources, define computer crime, describe the treatment of computer crimes in the Peruvian and comparative law, explain the spatial and temporal application of computer crimes, and point out the considerations of criminal policy; the research is qualitative-documentary Design; the Universe was the Criminal Law and the Computer Law, and the object of study the Computer Crimes; The methods used were: legal dogmatic, historical-comparative, inductive, deductive, analysis and synthesis; Among the most relevant results are the formulation of the Human Criminal Computer Law, as a derivation of the Human Criminal Law of the jurist Eugenio Raúl Zaffaroni, and we conclude in a general way, that the Human Criminal Computer Law, is the criminal legal knowledge that through the interpretation of laws criminal

on computer crimes, proposes to the legal agents a system to reduce the power of vigilance of punitive power in the control society and to promote the legal power in order to preserve the spaces of freedom and privacy of the people; and specifically that the limits or projection horizons of Computer Criminal Law, is explained by its own definition as legal knowledge, which aims to study legal security, and the criminal laws on Computer Crimes as an object of interpretation; it has the function of reducing the power of vigilance of punitive power; it is characterized by being public, repressive, continuous, fragmentative and normative; the interdisciplinarity of the Computer Law and the Criminal Law, is explained by its correspondence of juridical knowledge of secante form; also this criminal legal knowledge has sources of knowledge, information and production (in the case of criminal laws); on the spatial and temporal application, computer crimes are transnational, and that the Principles of temporary application of the Penal Code must be used; finally that the media criminalization, has fomented the computer crimes, and with it the punitive power and its power of vigilance are more potentiated, and that the Computer Crimes can be prevented.

Key Words: crime, informatics, society, punitive power, control.

I. INTRODUCCIÓN

1.1. CONSIDERACIONES GENERALES

La sociedad actual, es llamada Sociedad de la Información o Sociedad del Riesgo, en la que predomina el uso de las Tecnologías de la Información y Comunicación (TIC), fenómeno o paradigma social que es legitimado por el Derecho Informático y el Derecho Penal; el Derecho Informático proveyendo conocimientos conforme al avance científico, y el Derecho Penal estudiando los delitos informáticos con una asepsia política, sin preocuparse por definir o precisar los tipos penales; esta cuestión en la sociedad de control se hace peligrosa, pues mediante la criminalización primaria se ha incrementado el estado de vulnerabilidad de la población, dejándolo a merced del poder punitivo y su vigilancia, donde es posible divisar la actuación irracional de los agentes ejecutivos del sistema penal actuando por una selectividad estereotipada en una sociedad de control que legitima la intervención de los derechos fundamentales de las personas, sobreponiendo los intereses de la Seguridad Nacional sobre los derechos personales constitucionalmente válidos; por estas razones, justificamos la importancia de conceptuar un derecho penal informático deslegitimante del poder punitivo en la sociedad de control.

Por esta problemática, nos hemos propuesto definir el Derecho Penal Informático, para ofrecer al juzgador, al académico, y al legislador, una visión deslegitimante del poder punitivo que pervive escondido en la sociedad de la información, esta propuesta ayuda a revelar que nos encontramos en una Sociedad de Control, en la que el poder de vigilancia conculca la privacidad de los ciudadanos, y nos expone a un riesgo de perder nuestros espacios de libertad, y lo peor dejar que se edifique un Estado de Policía, que sin contención puede desencadenar genocidios.

También nos planteamos, explicar la necesaria interdisciplinariedad entre el Derecho Informático y el Derecho Penal, unificarlos en un único plan funcional, y entre otras metas, intentamos estudiar sus Fuentes, definir el Delito Informático, explicar el tratamiento de los Delitos Informáticos en el Perú, investigando su genealogía con el Derecho Comparado y finalizamos con algunas consideraciones desde la perspectiva de la Criminología Cautelar.

1.2. PLANTEAMIENTO DEL PROBLEMA

En las últimas décadas, la informatización de la sociedad, por el impacto de la Revolución Tecnológica (tecnología digital), ha nominalizado el mundo real como Sociedad Digital, trayendo consigo las Tecnologías de la Información y de la Comunicación (TIC), lo que implica positivamente, distancias reducidas, nuevas áreas de trabajo, satisfacción en el trabajo, productividad, liberación de las enormes cargas intelectuales del ser humano; y negativamente, incremento de los niveles de vigilancia sobre los movimientos, acciones y comunicaciones de todos los habitantes, la tecnificación del criminal, nuevos discursos de prevención y el reproche de conductas ofensivas a los sistemas de información, que potencian al poder punitivo con la llamada *Sociedad de Control*, que reduce los espacios de libertad y de privacidad de todos los habitantes.

Los fenómenos informáticos son contemplados por el Derecho Informático; y el Derecho Penal, ha considerado a las leyes penales manifiestas, no manifiestas y eventuales sobre delitos informáticos como nueva materia de interpretación.

Las leyes penales sobre delitos informáticos, no son bien definidos ni precisados, con la posibilidad de reducir espacios de libertad y de privacidad (sociedad de control), e imponer penas rechazando los datos del ser y la selectividad del poder punitivo, que incrementan el estado de vulnerabilidad de todos los habitantes.

1.3. FORMULACIÓN DEL PROBLEMA

1.3.1. PROBLEMA GENERAL:

¿Cuál es la naturaleza jurídica del Derecho Penal Informático?

1.3.2. PROBLEMAS ESPECÍFICOS:

1. ¿Cuál es el límite u horizonte de proyección del Derecho Penal Informático?
2. ¿Por qué es necesaria la interdisciplinariedad del Derecho Informático y el Derecho Penal?
3. ¿Cuáles son las Fuentes del Derecho Penal Informático?
4. ¿Qué es del Delito Informático?
5. ¿Cómo es el tratamiento de los Delitos Informáticos en el Derecho Penal peruano y comparado?
6. ¿Cómo es la aplicación espacial y temporal de los Delitos Informáticos?
7. ¿Cuáles son las consideraciones de Política Criminal sobre los Delitos Informáticos?

1.4. HIPÓTESIS DE LA INVESTIGACIÓN

1.4.1. GENERAL

El Derecho Penal Informático, es un saber jurídico penal, que mediante la interpretación de la ley penal sobre delitos informáticos construye un sistema que limita

el poder punitivo y normaliza la sociedad de control cautelando los nuevos espacios de libertad y de privacidad de la población.

1.4.2. ESPECÍFICOS:

El Derecho Penal Informático, es el saber jurídico-penal, que, mediante la interpretación de las leyes penales sobre delitos informáticos, propone un sistema orientador de decisiones que contiene y reduce el poder punitivo, para normalizar la sociedad de control e impulsar el progreso del Estado Constitucional de Derecho. El Derecho Penal Informático tiene por Universo, a las leyes penales sobre delitos informáticos, éstos son interpretados conforme a los conocimientos del Derecho Informático. El Derecho Penal Informático, es de carácter público, normativo, continuo, represivo y fragmentario del poder punitivo.

El Derecho Informático, explica los fenómenos de tecnificación de la información, la contempla como medio y objeto, y el Derecho Penal acotante, reduce y contiene el ejercicio del poder punitivo; ambas ramas de la ciencia jurídica, se corresponden por sus funciones diferentes.

El Derecho Penal Informático, como saber, tiene *Fuentes de Conocimiento* (leyes, informática, datos sociales, y otros) y *de Información* (tratados, manuales, artículos, etc.); y como objeto de interpretación (ley penal), tiene Fuentes de Conocimiento (leyes) y de Producción (órganos).

El *Delito Informático*, es definido de manera *formal*, como acción u omisión prohibida por la ley penal de delitos informáticos; *material*, conducta final que

contradice bienes jurídicos estudiados por el derecho informático, y *analítica*, como conducta, típica, antijurídica y culpable que tiene como medio u objeto a las TIC. El Delito Informático, tiene funciones, características y una clasificación, distinta de los delitos ordinarios.

El tratamiento de los delitos informáticos en el derecho peruano, está regulada por leyes penales manifiestas, latentes y eventuales, como la Ley 30 096; mientras que en el derecho comparado, se encuentra regulado por diversas leyes especiales heterogéneas, en varios países como España, Argentina, Ecuador, Alemania y Chile.

La aplicación espacial y temporal de las leyes penales sobre delitos informáticos, presenta dificultades por su carácter transaccional y los nuevos escenarios que presenta.

Los efectos de la criminalización de los delitos informáticos pueden ser nocivos sin la contención del poder punitivo en la sociedad de control, y que las disciplinas dedicadas a la informática y una política criminal adecuada, ayudan a la prevención de los delitos informáticos.

1.5. JUSTIFICACIÓN DEL ESTUDIO

La Investigación, se justifica en el cúmulo de conocimientos que se añaden acerca de los delitos informáticos, al plantear una dogmática jurídico - penal "deslegitimante" para los delitos informáticos, esto es, desvelar al poder punitivo en sus diversas manifestaciones en el tratamiento de los delitos informáticos conforme al derecho penal humano formulado por el jurista Eugenio Raúl Zaffaroni, con ello la tarea interpretativa de los operadores jurídicos tendrá una función limitativa de la coerción

que no es de carácter civil o administrativa, también la necesidad de contar con una explicación de la interdisciplinariedad secante del derecho penal y el derecho informático, para normalizar "la sociedad de control"; en otras palabras, la investigación ofrece un saber jurídico penal acotante del poder punitivo que se expresa con una intervención exacerbada en la esfera privada de la población fundados en discursos de seguridad paranoicos; pues creemos que el proceso de normalización de la sociedad de control efectuada por una práctica judicial orientada por el derecho penal informático, reduce la vulnerabilidad de la personas frente a la inevitable actuación del poder punitivo legitimado.

1.6. OBJETIVOS

1.6.1. GENERAL

Definir el Derecho Penal Informático.

1.6.2. ESPECÍFICOS:

Explicar los limites u horizonte de proyección del Derecho Penal Informático.

Explicar la interdisciplinariedad del Derecho Informático y el Derecho Penal.

Señalar las Fuentes del Derecho Penal Informático.

Definir el Delito Informático.

Describir el tratamiento de los Delitos Informáticos en el Derecho Penal peruano y comparado.

Explicar la aplicación espacial y temporal de los Delitos Informáticos.

Señalar las consideraciones de Política Criminal sobre los Delitos Informáticos.

II. REVISIÓN DE LITERATURA

2.1. ANTECEDENTES

A nivel Regional

Tesis de Miguel ARRARTE VERA: "El Derecho y la Tecnología Informatizada" para optar el Título de Abogado por la Universidad Nacional del Altiplano de Puno, sustentada el 05 de octubre del año de 1 999.

A nivel Nacional

Tesis de Luis Miguel REYNA ALFARO, "La Informática y su trascendencia jurídico penal: la Información como bien jurídico protegido", presentada en la Universidad de San Martín de Porres. Facultad de Derecho y Ciencias Políticas. Lima, en el año de 1 997, y publicada en el libro titulado *"Los delitos informáticos: Aspectos criminológicos, dogmáticos y de política criminal"* durante el año 2 002, por la Editorial Jurista Editores.

Tesis de Ángel Alfonso ARATA SALINA, para optar el Título Profesional de Abogado por la Universidad Nacional Mayor de San Marcos, titulada *"Las nuevas tecnologías de la información y la problemática jurídica del comercio electrónico"*.

A nivel Internacional

Tesis Profesional presentada por Pamela TRILLO MINUTTI, como requisito parcial para obtener el Título en Licenciatura en Derecho con área en Derecho Fiscal de la Universidad de las Américas Puebla, titulada *"Tipificación de los delitos informáticos y electrónicos en la Legislación Mexicana"*, esta investigación tuvo por objetivo general el análisis dogmático e interpretativo de la falta de fundamento teórico

y de estudio detallado de los elementos de los tipos penales de delitos electrónicos y delitos informáticos, los cuales vulneran los bienes jurídicos de la propiedad y de la privacidad.

Memoria de Alejandro ACOSTA PATRONI, presentada en marzo del 2 003, para optar el Grado de Licenciado en Ciencias Jurídicas y Sociales por la Universidad de Chile, titulada *"Hacking, cracking y otras conductas ilícitas cometidas a través de Internet"*.

2.2. MARCO TEÓRICO

1. LÍMITE U HORIZONTE DE PROYECCIÓN DEL DERECHO PENAL

El Derecho Penal, mediante un sistema de comprensión se encarga de la explicación de complejos normativos (normas jurídicas) que habilitan o limitan el ejercicio del poder coactivo estatal en forma de pena (poder punitivo), caracterizada por sanciones diferentes a las de otras ramas del saber jurídico (Zaffaroni, E. R., Slokar, A., y Aliaga, A., 2 011, p. 4).

1.1. DEFINICIÓN DEL DERECHO PENAL: El *Derecho Penal*, es la rama del saber jurídico que, mediante la interpretación de las leyes penales, propone a los jueces un sistema orientador de decisiones que contiene y reduce el poder punitivo, para impulsar el progreso del Estado Constitucional de Derecho (Zaffaroni, E. R., et al, 2 011, p. 5).

1.2. OBJETO: El objeto del Derecho Penal es la *seguridad jurídica*, porque tutela los derechos o bienes jurídicos de todos los habitantes frente a un poder

que podría ser ilimitado (Estado de Policía), al proponer a las agencias jurídicas que operen optimizando su ejercicio de poder controlar, limitar y reducir el poder de las agencias de criminalización primaria y secundaria (Zaffaroni, E. R., et al, 2 002, p. 80).

El Derecho Penal, tiene por objeto principal la interpretación a la *ley penal* (Zaffaroni, E. R. et al, 2 002, p. 97).

1.3. FUNCIÓN: Es la contención del poder punitivo, que es ejercido por la autoridad pública, esto es, recortar la intensidad, extensión, eliminar o evitar los actos verticales de mayor irracionalidad (Zaffaroni, E. R. et al, A., 2 011, p. 96).

1.4. CARACTERES DEL DERECHO PENAL (SABER PENAL):

a) Público, porque es una rama del Derecho Público que contiene al poder punitivo (Zaffaroni, E. R., et al, 2 011, p. 96-97).

b) Represivo, porque el poder punitivo necesita represión para posibilitar la civilización. El derecho penal debe operar como dique para represar las pulsiones irracionales del poder punitivo del Estado (Zaffaroni, E. R., et al, 2 011, p. 97).

c) Continuo y fragmentador, porque el Derecho Penal abarca todo el ejercicio del poder público (leyes penales manifiestas, latentes y eventuales) para identificar al poder punitivo que debe mantenerse discontinuo y fragmentario, sabiendo que el Derecho Penal debe contener su estructural tendencia a la

continuidad que sin la contención desembocaría en el Estado totalitario, fragmentarlo y acentuarlo en la medida del poder de las agencias judiciales (Cf. Zaffaroni, E. R., et al, 2 011, p. 81-82). Lo que es fragmentario y secundario es la ley penal manifiesta, porque recorta algunas conductas y las criminaliza en forma discontinua (Cf. Zaffaroni, E. R., et al, 2 002, p. 97).

d) Normativo, porque el Derecho Penal se ocupa de las leyes penales (normas penales reales, escritas y publicadas en el Diario Oficial (Cf. Zaffaroni, E. R., et al, 2 011, p. 83).

Cabe aclarar que el Derecho Penal (saber penal) no es sancionador por su función contendora del poder punitivo; sancionador es la ley penal manifiesta, y no es constitutivo, porque no crea bienes jurídicos (Cf. Zaffaroni, E. R., et al, 2 002, p. 98).

1.5. EQUIVOCIDAD:

Es indispensable distinguir:

a) Legislación penal o ley penal: La hace el legislador (agencia política: poder legislativo y el ejecutivo, previa delegación de facultades, mediante D.S. o D.L.).

b) Poder punitivo: Lo ejercen las agencias ejecutivas (policía).

c) Derecho penal: Lo elaboran los profesores y doctrinarios; estos programan son un sistema de filtración al poder punitivo.

1.6. PODER PUNITIVO:

Es todo ejercicio de coerción estatal, que no pertenece al derecho civil o privado, tampoco al administrativo, que en el imaginario social suele ser confundido con lo penal, ejemplo, la intervención policial para detener a quien nos corre con un cuchillo por la calle, es administrativa; lo penal comienza recién después que el sujeto ha sido detenido y el peligro para nosotros ha pasado. (Cf. Zaffaroni, E. R., et al, 2 011, p. 9).

El poder punitivo es: (a) *Manifiesto:* Habilitado por leyes penales manifiestas; y (b) *Latente o real:* Habilitado con cualquier pretexto (tutela de niños, internación geriátrica, servicio militar obligatorio, internación psiquiátrica, etc.). El poder punitivo latente se alivia con las garantías constitucionales.

2. LA INTERDISCIPLINARIEDAD DEL DERECHO PENAL

El conocimiento de un saber (o ciencia) no puede construirse sin el auxilio de otros saberes con los que se conecta en una red de interdisciplinariedad. Se trata de interdisciplinariedad constructiva de los saberes y no meras relaciones (y menos de vínculos de apoderamiento o de subordinación respecto de otras disciplinas); no hay ciencias auxiliares del Derecho Penal. Se trata de saberes que se superponen parcialmente con el objeto abarcado por el saber penal: Éstos son los saberes *secantes* (imaginemos círculos parcialmente superpuestos); o bien de saberes que no se

superponen con los entes que abarca el Derecho Penal, pero que se tocan de modo necesario para su precisión conceptual que son los saberes *tangentes* (imaginemos círculos que se tocan en un punto). Tanto los saberes secantes como los tangentes pueden ser jurídicos o no jurídicos. (Zaffaroni, E. R., et al, 2 011, p. 123-124).

3. FUENTES DEL DERECHO PENAL

3.1. FUENTES DE LA LEGISLACIÓN PENAL

En primera aproximación –dice el profesor Zaffaroni- puede entenderse por *Legislación Penal,* al conjunto de leyes que programan la decisión de conflictos mediante una coerción que priva de derechos o infiere un dolor (pena) sin perseguir un fin reparador ni de neutralización de un daño en curso o de un peligro inminente (Zaffaroni, E. R., et al, 2 002, p. 37).

La legislación penal abarca las leyes penales manifiestas, latentes y eventuales, éstas pueden ser constitucionales (irracionalidad relativa: Irracionales pero lícitas) o inconstitucionales (irracionalidad grosera: Irracionales e ilícitas) (Zaffaroni, E. R., et al, 2 002, p. 101).

3.1.1. FUENTES DE CONOCIMIENTO DE LA LEGISLACIÓN PENAL:

Son las que nos permiten conocer la ley penal (Cf. Zaffaroni, E. R., et al, 2 011, p. 87 y Cf. Zaffaroni, E. R., et al, 2 002, p. 101).

3.1.2. FUENTES DE PRODUCCIÓN DE LA LEGISLACIÓN PENAL:

Son los órganos de los que emanan o producen las leyes penales (Cf. Zaffaroni, E. R., et al, 2 011, p. 87 y Cf. Zaffaroni, E. R., et al, 2 002, p. 101).

3.2. FUENTES PROPIAMENTE DICHAS DEL DERECHO PENAL

A) FUENTES DE CONOCIMIENTO DEL DERECHO PENAL: Son los datos que debe tomar en cuenta el saber penal para elaborar sus construcciones (Constitución, tratados internacionales, leyes penales formales, leyes penales materiales, leyes no penales, datos sociales y de otras disciplinas, información histórica, derecho comparado, jurisprudencia, filosofía, etc.). (Zaffaroni, E. R., et al, 2 011, p. 87; Zaffaroni, E. R., et al, 2 002, p. 102).

B) FUENTES DE INFORMACIÓN DEL DERECHO PENAL: Son las que permiten conocer el estado presente o pasado de este saber (tratados, manuales, compendios, cursos, enciclopedias, comentarios, artículos, revistas especializadas, monografías, ensayos, etc.) (Zaffaroni, E. R., et al, 2 011, p. 87; Zaffaroni, E. R., et al, 2 002, p. 102).

4. EL DELITO

El Delito es una conducta típica, antijurídica y culpable (Zaffaroni, E. R., 2 009a, p. 61, 71; Muñoz Conde, F., 1 999, p. 32).

5. TRATAMIENTO DE LOS DELITOS EN EL DERECHO PERUANO

CÓDIGO PENAL DE 1 991

En el Perú se tiene el Código Penal de 1 991, sancionado mediante Decreto Legislativo 635; es de concepción finalista, presenta influencia alemana, suiza y brasileña, reflejada en el sistema de penas, el error de tipo legal y error de prohibición (Hurtado Pozo, 2 011, p.119-121); tuvo la intención de

adecuarse a la Constitución de 1 979 y esbozó el error de comprensión culturalmente condicionado propuesto por los profesores Eugenio Raúl Zaffaroni, Raúl Peña Cabrera y Felipe Villavicencio Terreros.

6. TRATAMIENTO DE LOS DELITOS EN EL DERECHO COMPARADO

6.1. ESPAÑA. CÓDIGO PENAL DE 1 995: España cuenta con un Código Penal vigente con la sanción de la Ley Orgánica 10/1 995, que viene a ser una respuesta a las tendencias de constitucionalización de los Ordenamientos Jurídicos en nuestro planeta con la reforma de la pena y otras instituciones penales conforme a los valores constitucionales.

6.2. ARGENTINA. CÓDIGO PENAL DE 1 921: La Ley 11.179 sancionó el vigente Código Penal argentino, a decir del profesor Zaffaroni, abolió la pena de muerte e introdujo la condenación y la libertad condicionales, supo escapar a la influencia positivista del ambiente, siendo escueto y racional (Cfr. Zaffaroni, E. R., et al, 2 002, p. 252).

6.3. ECUADOR. CÓDIGO ORGÁNICO INTEGRAL PENAL DEL 2 014: Se trata de un cuerpo normativo que reúne la parte sustantiva, adjetiva y ejecutiva del Derecho Penal, entorno a mandatos imperativos de la Constitución Ecuatoriana del 2 008; este Código tiene como finalidad normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas

con estricta observancia del Debido Proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas.

6.4. ALEMANIA. CÓDIGO PENAL ALEMÁN DE 1 872 CON LA REFORMA DE 1 974 Y 1 998: El jurista alemán Hans Welzel, comenta que sobre la base de este Código Penal (Strafgesetzbuch) se desplegó una rica vida científica, que cristalizó alrededor de dos Escuelas. Los "clásicos", con Binding a la cabeza, guardaron la ideología conservadora autoritaria, delimitada por el Estado jurídico, y la idea de la retribución, que juntas habían determinado el ambiente espiritual del C.P., como herencia del idealismo de Kant y Hegel (Welzel, H. 1 956, p. 18).

7. DIMENSIÓN ESPACIAL Y TEMPORAL DE LOS DELITOS

7.1. VALIDEZ ESPACIAL DE LA LEY PENAL: El Derecho Penal, es el sistema interpretativo de leyes que rigen en determinado espacio que, en principio, es el territorio del Estado (territorialidad) (Zaffaroni, E. R., 2 009, p. 50). Se determina con los siguientes principios: a) Principio de ubicuidad del delito, b) Principio de territorialidad, c) Principio del pabellón (derecho de bandera), d) Principio de extraterritorialidad, e) Principio real o de Defensa (de protección de intereses), f) Principio de personalidad o de nacionalidad, g) Principio de personalidad activa, h) Principio de personalidad pasiva, i) Principio de universalidad (justicia mundial) (Rubio Correa, M., 2 009, p. 301 y ss.).

7.2. ÁMBITO DE VALIDEZ TEMPORAL DE LA LEY PENAL. *TEMPUS REGIT ACTUM* (EL TIEMPO RIGE LOS ACTOS): En el caso de sucesión de leyes penales en el tiempo, el juicio de aplicación de la ley penal en abstracto al caso concreto inicia determinando el momento en el que se inició el curso causal (Art. 9 del C. P), y se pueden aplicar los Principios de Aplicación inmediata o irretroactividad de la ley penal, Aplicación retroactiva, Aplicación ultractiva, Principio de combinación de leyes penales, *lex tertia.*

8. POLÍTICA CRIMINAL

A decir de Hulsman, la *"política criminal"* es a menudo entendida como "la política en relación al delito y a los delincuentes". (1 993, p. 82), esto se entiende de manera más clara con el profesor Hurtado, para quien la Política Criminal es la actividad del Estado dirigida a enfrentar las acciones delictuosas (*lato sensu*) que amenazan la cohesión y el desenvolvimiento armónico de la comunidad. (Hurtado Pozo, J., 2 011, p. 51).

Otra de las cuestiones a tomar en cuenta es la *Prevención del Delito*, entendida como el conjunto de programas, servicios y acciones que tienen por objeto el mejoramiento del entorno social. (Herrera Pérez, A., 2 002, p. 79). Al respecto el profesor Claus Roxin, opina que debido a la restringida eficacia de la pena y, también, a su nocividad, se debe dedicar mayor atención a la prevención del delito a través de medios de política social, policiacos, legislativos y técnicos. (Roxin, C., 2 002, p. 94).

2.3. MARCO CONCEPTUAL

1. DERECHO PENAL: El *Derecho Penal*, es la rama del saber jurídico que, mediante la interpretación de las leyes penales, propone a los jueces un sistema orientador de decisiones que contiene y reduce el poder punitivo, para impulsar el progreso del Estado Constitucional de Derecho. (Zaffaroni, E. R., et al, 2 002, p. 5).

2. DERECHO INFORMÁTICO: Es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática) (Téllez Valdez, 2 008, p. 9.).

3. DESLEGITIMACIÓN: *"Des"*, es un prefijo que denota negación o inversión del significado simple, y *"Legitimar"*, es probar o justificar la verdad de algo o la calidad de alguien o algo conforme a las leyes, también, habilitar a alguien, de suyo inhábil, para un oficio o empleo (RAE, 2 003). En síntesis, *deslegitimar* es negar la legalidad o inhabilitar algo, ese algo es el poder punitivo; por el contrario, *legitimar* es pretender caracterizar de racional algo que es utópicamente legítimo, como el sistema penal, que a decir del profesor Zaffaroni, es una compleja manifestación del poder social. (Zaffaroni, E. R., 1 998, p. 20).

4. PODER PUNITIVO: Es todo ejercicio de coerción estatal, que no pertenece al derecho civil o privado, tampoco al administrativo, que en el imaginario social suele ser confundido con lo penal, ejemplo: La intervención policial para detener a quien nos corre con un cuchillo por la calle, es administrativa; lo penal

comienza recién después que el sujeto ha sido detenido y el peligro para nosotros ha pasado (Zaffaroni, E. R., 2 011, p. 9).

5. SOCIEDAD DE CONTROL: Es una sociedad totalitaria en la que un reducido número de personas impone medidas y conductas al resto y en la que esta imposición es posible debido a un estricto control de lo que los ciudadanos pueden hacer de forma individual (Alcántara, J., 2 008, p. 102-103).

III. METODOLOGÍA

3.1. DISEÑO Y TIPO DE INVESTIGACIÓN

La presente investigación corresponde al Diseño cualitativo-documental, de Tipo jurídico-dogmático.

3.2. ÁMBITO O LUGAR DE ESTUDIO

El ámbito de estudio es el Derecho Penal y el Derecho Informático.

3.3. UNIVERSO Y MUESTRA

En el presente trabajo, el Universo está compuesto por el Derecho Penal y el Derecho Informático, y como Muestra u objeto de estudio, a los Delitos Informáticos en el Perú, Ecuador, Argentina, España, Alemania y Estados Unidos.

3.4. DESCRIPCIÓN DE MÉTODOS POR OBJETIVOS ESPECÍFICOS

A continuación, se detallan los métodos a emplearse en cada objetivo de la investigación.

1. DEFINIR EL DERECHO PENAL INFORMÁTICO

Los Métodos que se utilizan para el estudio de la información son: El análisis-síntesis, inducción-deducción, dialéctico y comparativo. La Técnica de recolección de datos, es el análisis documental, mediante las fichas textuales como instrumento.

Los Indicadores de la dimensión: Límites u horizonte de proyección del Derecho Penal Informático, a ser definidos son:

a) Definición

b) Objeto

c) Función

d) Caracteres.

2. EXPLICAR LA INTERDISCIPLINARIEDAD DEL DERECHO INFORMÁTICO Y EL DERECHO PENAL:

Los Métodos utilizados para el estudio de la información, son: El análisis-síntesis, inducción-deducción, dialéctico y comparativo.

La Técnica de Recolección de datos, es la técnica del análisis documental, mediante las fichas textuales como instrumento.

Los Indicadores de la dimensión: La necesaria interdisciplinariedad secante entre el Derecho Informático y el Derecho Penal, a ser explicados son:

a) Derecho Informático.

b) Derecho Penal.

c) La correspondencia entre saberes jurídicos.

3. SEÑALAR LAS FUENTES DEL DERECHO PENAL INFORMÁTICO

Los Métodos utilizados para el estudio de la información, son: El análisis-síntesis, inducción-deducción, dialéctico y comparativo.

La Técnica de recolección de datos es el análisis documental, mediante las fichas textuales como instrumento.

Los Indicadores de la dimensión: Fuentes del Derecho Penal Informático, a ser señalados son:

a) Del Derecho Penal (conocimiento e información).

b) De la legislación penal (conocimiento y producción).

4. DEFINIR EL DELITO INFORMÁTICO

Los Métodos utilizados para el estudio de la información, son: El análisis-síntesis, inducción-deducción, dialéctico y comparativo.

La Técnica de recolección de datos es el análisis documental, mediante las fichas textuales como instrumento.

Los Indicadores de la dimensión: El Delito Informático, a definir son:

a) Definición (Formal, Material, Analítica).

b) Funciones.

c) Características.

d) Clasificación.

5. DESCRIBIR EL TRATAMIENTO DE LOS DELITOS INFORMÁTICOS EN EL DERECHO PERUANO Y COMPARADO:

Los Métodos que se utilizan para el estudio de la información son: El histórico-comparativo, análisis-síntesis, inducción-deducción, dialéctico y comparativo.

La Técnica de recolección de datos es el análisis documental, mediante las fichas textuales como instrumento.

Los Indicadores de la dimensión: Tratamiento de los Delitos Informáticos en el Derecho peruano y comparado, a ser descritos son:

a) Delitos contra Datos y Sistemas Informáticos

b) Delitos Informáticos contra la Indemnidad y Libertad Sexuales

c) Delitos Informáticos contra la Intimidad y el Secreto de Las Comunicaciones

d) Delitos Informáticos contra el Patrimonio

e) Delitos Informáticos contra la Fe Pública

f) Abuso de mecanismos y dispositivos informáticos.

6. EXPLICAR LA APLICACIÓN ESPACIAL Y TEMPORAL DE LOS DELITOS INFORMÁTICOS

Los Métodos utilizados para el estudio de la información son: El análisis-síntesis, inducción-deducción, dialéctico y comparativo.

La Técnica de recolección de datos es el análisis documental, mediante las fichas textuales como instrumento.

Los Indicadores de la dimensión: Dimensión temporal y espacial de los Delitos Informáticos, a ser explicados son:

a) Aplicación espacial de la ley penal

b) Aplicación temporal de la ley penal

7. SEÑALAR LAS CONSIDERACIONES DE POLÍTICA CRIMINAL SOBRE LOS DELITOS INFORMÁTICOS:

Los Métodos utilizados para el estudio de la información, son: El análisis-síntesis, inducción-deducción, dialéctico y comparativo.

La Técnica de recolección de datos, es la técnica del análisis documental, mediante las fichas textuales como instrumento.

Los Indicadores de la dimensión: Consideraciones de Política Criminal sobre los Delitos Informáticos, a ser señalados son:

a) Política criminal y los delitos informáticos.

b) Prevención de los delitos informáticos.

3.5. OPERACIONALIZACIÓN DE VARIABLES

TABLA DE OPERACIONALIZACION DE LAS VARIABLES

Variable /Unidad / eje temático	Dimensión	Indicador	Método	Técnica	Instrumento
Derecho Penal Informático	1. Límites u horizontes de proyección del Derecho Penal Informático.	1.Definición 2. Objeto 3.Función 4.Caracteres.	1.Método jurídico (Dogmático-jurídico). 2. Analítico 3. Sintético 4. Comparativo.	1. Investigación documental (Análisis e interpretación de contenido).	1. Ficha textual.
	2. La necesaria interdisciplinariedad secante entre el Derecho Informático y el Derecho Penal.	1.Derecho Informático. 2.Derecho Penal. 3.La correspondencia entre saberes jurídicos.			
	3. Fuentes del Derecho Penal Informático.	1. Del Derecho Penal. (conocimiento e información). 2.De la legislación penal (conocimiento y producción)			
	4. El Delito Informático.	1. Definición (Formal, Material, Analítica) 2.Funciones.			

		3.Características. 4. Clasificación. 5. Sujetos.			
	5. Tratamiento de los Delitos Informáticos en el Derecho peruano y comparado.	1. Delitos contra Datos y Sistemas Informáticos 2. Delitos Informáticos contra la Indemnidad y Libertad Sexuales 3.Delitos Informáticos contra la Intimidad y el Secreto de las Comunicaciones 4. Delitos Informáticos contra el Patrimonio 5.Delitos Informáticos contra la Fe Pública 6. Abuso de mecanismos y dispositivos informáticos			
	6.Dimensión espacial y temporal de los Delitos Informáticos.	1. Aplicación espacial de la ley penal 2. Aplicación temporal de la ley penal.			
	7. Consideraciones de Política Criminal sobre los Delitos Informáticos.	1. Política Criminal y los Delitos Informáticos 2. Prevención de los Delitos Informáticos.			

IV. RESULTADOS Y DISCUSIÓN

4.1. LÍMITES U HORIZONTE DE PROYECCIÓN DEL DERECHO PENAL INFORMÁTICO

§ 1. DEFINICIÓN

1. El Derecho Penal Informático, es el *saber jurídico penal que, mediante la interpretación de leyes penales sobre delitos informáticos, propone a los agentes jurídicos un sistema reductor del poder de vigilancia del poder punitivo en la sociedad de control e impulsar el poder jurídico con el fin de preservar los espacios de libertad y privacidad de las personas*. Cabe precisar que la expresión Derecho Penal Informático, al igual que la rama principal (Derecho Penal), tiene varios sentidos, como: Doctrina, legislación de delitos informáticos, ejercicio coactivo (poder punitivo), a lo que nos referimos al inicio, es al primer sentido, que se traduce en un intento de ofrecer una explicación o un sistema de comprensión del resto de sentidos, esto es, la ley penal y el poder punitivo.

2. Es un saber jurídico penal, porque es un programa técnico-político del derecho penal humano, que como tal busca el conocimiento acerca de los delitos informáticos para formular discursos que orienten las decisiones judiciales en un marco de poder político y económico, por tanto, aspira a ser un programa de doctrina jurídico-penal que se convierta en jurisprudencia en asuntos de delitos asociados a las Tecnologías de la Información y la Comunicación.

3. El método dogmático deslegitimante del derecho penal humano, permite la construcción de un sistema orientador, a los jueces para dictar sentencias judiciales, a

los fiscales y abogados para la formulación de tesis de imputación y de defensa, que se realizan mediante la interpretación de leyes penales sobre delitos informáticos, con la finalidad de limitar el poder de vigilancia del poder punitivo que es ejercido por las agencias ejecutivas (policías) y políticas (parlamentarios), y preservar el Estado Constitucional de Derecho.

4. En el año 2 016, el jurista Raúl Zaffaroni, afirmó que el poder de vigilancia del poder punitivo se practica sobre la gran mayoría de la población, con motivo o pretexto de tutela o protección frente al delito o a cualquier otra amenaza, la cual es aceptada por la población, por considerarse protegida, pero en realidad lo que le interesa al poder político y económico (sobre el poder punitivo), es vigilar con la tecnología de control, que reduce progresivamente la privacidad.

5. La vigilancia de la ciudadanía en nombre de la seguridad, mediante las tecnologías de control (Internet, RFID, video vigilancia, DRM, interceptación, etc.), y medidas legales (delitos informáticos, retención de datos, propiedad intelectual, etc.), es la denominada sociedad de control, que parte del binomio sociedad digital y vigilancia (Alcántara, J. F., 2 008, p. 35-38,102).

6. La sociedad de control, se vale de las tecnologías de control que son utilizadas sobre el flujo de la información (restricciones) y sobre las personas (fronteras) (Alcántara, J. F., 2 008, p. 130-137); si bien, es práctica común en Gobiernos totalitarios vigilar a los ciudadanos, con el ataque terrorista del 11 de setiembre de 2 001 en Estados Unidos de Norte América, la conciencia por la seguridad se intensificó tanto, que los países democráticos gestionan la seguridad con dispositivos de vigilancia en el

marco de una guerra global contra el terrorismo, basadas en una doctrina de la seguridad nacional (propio del Estado Policía) (Mattelart, A., 2 002, p. 160; Mattelart, A., 2 009; The Economist, 2 008, p. 53), que es una maquinación de la cultura del terrorismo que se ha desarrollado entre nosotros, como una estructura de poder, premunida de un arsenal de dispositivos e instituciones que dominan la vida social, política y económica de los ciudadanos (Chomsky, N., 1 998).

7. Después del 11 de setiembre, el Congreso de los Estados Unidos, sancionó la Ley Patriota (Patriot Act), la cual confiere poderes de vigilancia a las autoridades del orden público como el monitoreo del tráfico de Internet sin orden judicial, también el Pentágono desarrolló un sistema para investigar las transacciones electrónicas para detectar actividades sospechosas, de este modo tácitamente el Internet o la misma informática se ha convertido en una instrumento público omnipresente para el poder de vigilancia. (The Economist, 2 008, p. 45, 53).

8. En efecto, la informática, juega un papel importante en la sociedad de control, pues le permite a los Gobiernos recopilar información para mejorar la conexión entre organismos gubernamentales, y sobre todo para evitar un "Perl Harbor electrónico", que se trata de supuesto alarmista formulado por Richard Clarke, que consiste en un ataque terrorista a la infraestructura crítica de telecomunicaciones, electricidad y servicios públicos, paralizando a todo Estados Unidos (The Economist, 2 008, p. 45, 54).

9. La paranoia de los Estados Unidos, se extendió a toda la orbe, insuflando una gran preocupación por combatir la delincuencia informática en el resto de la periferia[1],

1 Para Armand Mattelart, Estados Unidos es el foco de la innovación tecno científicay la cultura de masas, producto de un modelo de consumo elevado, y es la primera sociedad global de la historia. (2

lo cual ocasionó el auge del panóptico global del poder punitivo sobre la sociedad digital o la denominada sociedad global de la información (Mattelart, A., 2 002, p. 143; Espinoza Coila, M., 2 014); de este modo, la convergencia del miedo y de la informática dieron origen a la sociedad de control, como un nuevo horizonte planetario gobernado y vigilado por unos cuantos que son tributarios de agencias nacionales de seguridad e inteligencia, a guisa de ejemplo, son las revelaciones de Edward Snowden (Mac Askill, 10 de junio de 2 013), ex empleado de la CIA y de la NSA (National Security Agency), quien declaró que la NSA ha construido una infraestructura que le permite interceptar casi todo (correos electrónicos, contraseñas, registros telefónicos, tarjetas de crédito), prácticas que a decir de Armand Mattelart, son parte del Sistema de Inteligencia Global, orientadas a interceptar con toda impunidad las comunicaciones de cualquier sospechoso. (2 002, p. 142).

10. En el año 2 002, Mattelart, al tratar la sociedad de la información, señaló que la *información* se convierte en el elemento fundamental de la hegemonía mediante las tecnologías de recogida de información e inteligencia, para poder competir con los rivales y anticipar las estrategias de las grandes organizaciones de la sociedad civil (p. 167), esta hegemonía por el poder de vigilancia, fue descrita por Michel Foucault (2 002), como la utopía de la ciudad perfectamente gobernada a través del poder disciplinario con la ayuda del panóptico de Bentham, quien ha sentado el Principio de que el poder debía ser visible e inverificable, pues el panóptico, siendo una torre con anillo periférico, puede ser fácilmente visto, sin que sea visible el observador que se encuentra detrás de las ventanas.

2002, p. 100), fuera de este centro Latinoamérica, es solo una periferia que gira en torno a este país.

11. Si el poder disciplinario tratado por Foucault se ejercía con el panóptico en un sistema cerrado, es con Gilles Deleuze (1 999), que en la sociedad de control, el poder de vigilancia actúa al aire libre, con un nuevo panóptico difuso, esto es, que es visible a través de organizaciones internacionales, agencias de seguridad e inteligencia de los Gobiernos, e inverificable con la ayuda de las tecnologías de control compuestas de equipos informáticos que son parte de las llamadas Tecnologías de la Información y de la Comunicación (TIC).

12. Giovanni Sartori, señalaba que las nuevas fronteras para el *homo sapiens* son Internet y el ciberespacio, además, nos advertía de la conversión del demo-poder a demo-impotencia en la ciberdemocracia o democracia electrónica que nos prometen las TIC, traducidas prácticamente en una infinita libertad (2 004, p. 57, 179), que con la intervención del poder de vigilancia resulta una entelequia, pues siendo los sistemas de información y datos informáticos, bienes jurídicos de relevancia penal, la criminalización primaria ha dado origen a los delitos informáticos, de este modo el legislador franqueó el poder punitivo hacia la soñada ciberdemocracia que conlleva una sociedad digital, amplificando el poder de vigilancia hasta alcanzar la sociedad de control, en la que las tecnologías de la información y comunicación, permiten que el panóptico del poder punitivo no tenga límites territoriales. (Espinoza Coila, M., 2 014; Requena Hidalgo, J., 2 004).

13. Ahora bien, la sociedad de control, nos conduce a consentir, lo que afirma José Hurtado Pozo: *Toda actividad en el ámbito de internet está sometida al Derecho Penal*, y agrega que para evitar problemas penales, cada uno debe comportarse en internet como lo hace en la vida cotidiana (2 017); por ello, ahora es momento de

preguntarnos qué Derecho Penal debe ocuparse de los delitos informáticos, mejor dicho qué dogmática penal es la más apropiada para el tratamiento de los delitos informáticos y la reducción del poder punitivo, y así evitar que éste se desborde y se asiente un Estado de Policía.

14. Conforme a la actual discusión del Derecho Penal (Polaino Navarrete, M., 2 008, p. 267-326; Zaffaroni, E. R., et al, 2 011, p. 261-273, 296-305), permítanos prescindir de la descripción del Finalismo de Hans Welzel[2], del Normativismo Moderado de Claus Roxin, y del Normativismo Radical de Günther Jakobs, por cuanto las disquisiciones que giran en torno a sus posturas, se circunscriben para la presente investigación, a que éstas, no obstante que se distingan de su naturaleza ontológica y neokantiana, todas terminan legitimando el poder punitivo, por ende aceptando el poder de vigilancia que impulsa el establecimiento de una sociedad de control, me explico, el Derecho Penal que desarrollaron se orientó a negar al Estado Real y las manifestaciones del poder punitivo, presentando un Estado Ideal, inexistente, el cual supuestamente se haría realidad con la protección de bienes jurídicos, el mantenimiento de la vigencia de la norma, y el trato diferenciado entre ciudadanos y enemigos, ficciones que se confunden entre el ser y el deber ser, lo cierto es, que los Estados reales, son procesos de ordenación y armonización de fuerzas sociales e individuales en desarrollo (Espinoza Coila, M., 2 013), donde urge consolidar los derechos humanos.

15. Consideramos necesario ocuparnos de algunas construcciones teóricas que han emergido con ocasión de la criminalidad organizada, altos crímenes de riesgo y los

2 El jurista español Miguel Polaino Navarrete (2008), refiere que del finalismo se han formulado algunas construcciones peculiares, que aceptando sus postulados básicos, critican algunos aspectos esenciales del finalismo, estos son: a) la construcción teleológica de Schmidhäuser, b) el derecho penal orientado a las ciencias sociales de la escuela de Frankfurt, c) el moderno normativismo neokantiano (Escuela de E.A. Wolff) y d) la corriente normativista de Frisch.

genocidios, que comprenden la cibercriminalidad, éstos son: (a) El Derecho Penal de la Seguridad de Urs Kindhäuser, (b) El Derecho Penal Preventivo de Ulrich Sieber, y (c) El Derecho Penal Humano de Raúl Zaffaroni.

16. (a) *El Derecho Penal de la Seguridad*, legitima al poder punitivo recurriendo al Derecho Penal como un instrumento de control social que procura la seguridad, para ello acorta o renuncia a las exigencias probatorias, protección de bienes jurídicos individuales, fines tradicionales de la pena, culpabilidad por el hecho individual, comprensión liberal del ser humano (miedo social) y emplea una política criminal simbólica (renuncia a la intervención mínima), pues como sostiene Kindhäuser (2 014), en una sociedad en camino de progreso (técnico) que genera múltiples peligros (sociedad del riesgo), la búsqueda de seguridad es legítima y es un derecho humano que justifica en importante medida la existencia del Estado y su monopolio de la violencia, afirmación poco feliz, si la seguridad por la desconfianza en los ciudadanos (o digamos enemigos del Estado), es usado como fundamento por Gobiernos totalitarios, en la que poco o nada interesa respetar los derechos individuales, pues están primero los intereses del Estado, entre comillas, porque son los intereses del proyecto político de facto los que prevalecen.

17. (b) *El Derecho Penal Preventivo*, nos ofrece el paradigma de la prevención y la seguridad para la protección de los intereses sociales en la sociedad del riesgo, y establece como límite del derecho penal: Los derechos humanos y el derecho constitucional (ponderación y el Principio de proporcionalidad) (Sieber, U., 2 015), desde su perspectiva preventiva y proteccionista de los intereses sociales, extiende la inteligencia secreta, mediante agentes encubiertos, interceptación de

telecomunicaciones, búsqueda de información en línea mediante software forense, vigilancia por audio y video, y análisis de datos, todo con autorización judicial, empero, no busca la contención del ejercicio del poder punitivo, dado que la combinación del discurso de los derechos humanos y la vigilancia, es bastante peligroso puesto que, esta teoría se fundamenta en un Estado de ficción, donde el control judicial es efectivo y los derechos humanos se respetan, es decir, un Estado ya realizado, o digamos plenamente desarrollado, y olvida que la protección de los intereses sociales y la pretendida dominación del poder de vigilancia del poder punitivo, es propio de Estados Autoritarios que se encubren en el discurso de los derechos humanos, en ese sentido, esta posición doctrinaria permitiría ingresar el poder punitivo en forma de Caballo de Troya a los Estados, consiguiendo actuar sin ser descubierto y la aceptación de la población, pues aparentemente se trataría de medidas autorizadas por el Poder Judicial y respetuosas de los derechos humanos, como sucedió con la NSA, que espiaba con el aval del gobierno de los Estados Unidos, y bajo autorización judicial, hasta que Snowden, reveló que esto no era cierto, que en realidad se había evitado el control judicial, y que vigilar a una persona implicaba analizar una cadena de datos de miles de personas, por ello esta teoría también resulta inadmisible.

18. Ambas Teorías, la del peligro y la preventiva, se ocupan de la sociedad del riesgo, la cual según la Tesis de Ulrich Beck, contiene una tendencia a un totalitarismo «legítimo» en la defensa contra peligros, el cual con el pretexto de impedir lo peor crea lo peor todavía (1 998, p. 88); porque el riesgo se puede entender como principio de activación de la civilización o en su extremo opuesto como barbarie (2 000, p. 79-80), en este caso, la inseguridad o los potenciales peligros han generado el Derecho Penal de Riesgo que, como señala el maestro Zaffaroni, pretende crear una sensación de

seguridad, luego desemboca en un Estado Preventivista, que ahoga al Estado de Derecho, confundiendo prevención policial con represión penal, reemplazando la ofensividad por el peligro y reduciendo los riesgos permitidos, asimismo, convierte los delitos de lesión en delitos de peligro, eliminando el *indubio pro reo,* cuando no se puede probar la producción del resultado, también sostiene que este derecho penal del riesgo simbólico, no neutraliza los riesgos; sino que le hace creer a la gente que ya no existen, se calma la ansiedad, se miente, convierten al derecho penal en una campaña publicitaria fraudulenta (2 011, p. 270), por ello, toda teoría pura o ecléctica que opere sobre una Estado de ficción de seguridad total o de riesgo, renunciando a los derechos humanos y al control judicial, o peor que mediante una alquimia entre ellas, pretenda dominar plenamente al poder punitivo, por consiguiente resulta una dogmática penal ponzoñosa para el tratamiento de los delitos informáticos y la contención del poder punitivo en la sociedad de control.

19. La tarea de preservar los espacios de libertad y la privacidad de las personas, implica la contención del poder de vigilancia del poder punitivo que se habilitan con los delitos informáticos, con una dogmática deslegitimante del poder de policía, es decir, de un derecho penal que reduzca los estados de vulnerabilidad de la población frente al poder punitivo, además que no acepte el estado normal de cosas, sin preguntarse un para qué y un por qué, que guarde coherencia normativa, fáctica y políticamente humana, que posibilite el avance de los derechos humanos, acepte los datos de la realidad, baje los niveles de vulnerabilidad de los más desfavorecidos, siendo consciente de su operación dentro de una marco de poder político y económico, y de su imposibilidad de regular el poder punitivo, y que solo puede y debe contener y reducir el poder punitivo, pero no desaparecerlo, pretender ello significa desviarse hacia un romanticismo penal

forjado en la ilusión de solucionar los problemas de la sociedad. (Zaffaroni, 2 016 y 2 011, p. 282).

20. (c) En el 2 016, el jurista Raúl Zaffaroni, presentó el modelo del *derecho penal humano*, y sostiene que éste debe preservar cuidadosamente los espacios de libertad que permitan el desarrollo de la dinámica política, social y económica de nuestras sociedades, y que a través de la profundización de la constitucionalización e internacionalización del derecho penal bajo la premisa básica de que todo ser humano es persona, necesariamente desembocará en el privilegio de la vida frente a la amenaza de su destrucción masiva y, por ende, asumirá por mandato jurídico positivo su función de prevención del genocidio y de protección de todos los bienes jurídicos.

21. El tratamiento de los delitos informáticos, no puede eludir los principios de la centralidad de la persona humana y del bien común, que nos encaminan hacia un auténtico desarrollo humano y el cuidado de la hermana madre tierra, que son cuestiones preocupantes en nuestro tiempo de globalización (Benedicto XVI, 2 009, p. 76, 32; Francisco, 2 015; DW, 2 017, June 2), por ello, sin ambages el derecho penal informático, ha de tener necesariamente sus raíces en el derecho penal humano que impulsa la realización del programa constitucional y que incorpora datos de la realidad social, en consecuencia debe adoptar su objeto, función, caracteres, fuentes y su interdisciplinariedad con otros saberes, a efecto que sea parte de un mismo *corpus* reductor del poder punitivo y constitucionalizado, conforme a la premisa de que todo ser humano es una persona.

22. En el año 2 014, el citado jurista Zaffaroni, describió la pulsión que existe entre el derecho penal humano y el inhumano, señalando que el lado humano, procura configurar modelos de sociedades incluyentes, que reduzcan la estratificación mediante cierto grado de redistribución de la renta y aumentando la base de ciudadanía real, en tanto que, el lado, inhumano está dominada por el poder financiero, que procura reforzar y aumentar la posición de quienes llevan la mejor parte en la distribución y mueven poderosos factores de poder hacia un derecho inhumano.

23. En ese orden de ideas, prescindir del modelo del derecho penal humano en la construcción de un sistema de comprensión de los delitos informáticos, significaría decantar por inercia al derecho penal inhumano que busca expandir el poder punitivo fabricando enemigos para facilitar el genocidio por goteo, configurando un Estado vigilantista omnividente, que se legitima con un sistema penal políticamente neutro, sistémico u organicista. (Zaffaroni, E. R., 2 016; Zaffaroni, E. R., 2 014). De este modo, divisamos un derecho penal informático humano y otro inhumano, que describimos en la Tabla 1 que sigue.

TABLA 1

Comparación entre el derecho penal informático humano e inhumano

Derecho Penal Informático Inhumano
El derecho penal informático inhumano, legitima la sociedad de control, donde el poder de vigilancia del poder punitivo es aceptada por la población por la ilusión de obtener mayor seguridad y combatir el terrorismo global, discurso que permite la desmesurada habilitación del poder punitivo, con leyes penales sobre delitos informáticos, que no son bien definidos ni precisados, con la posibilidad de reducir espacios de libertad y de privacidad, e imponer penas rechazando los datos del ser y la selectividad del poder punitivo, que incrementan el estado de vulnerabilidad de todos

los habitantes, especialmente de los más débiles, de modo que cualquier Gobierno podría establecer un régimen autoritario con el pretexto de garantizar la seguridad nacional motivado por la cultura del terrorismo con el riesgo de encubrir genocidios.

Derecho Penal Informático Humano

El Derecho Penal Informático personalizado por el Derecho Penal Humano de Zaffaroni, deslegitima la sociedad de control, donde el poder de vigilancia del poder punitivo es reducida a límites inferiores (no desaparecida) para atenuar los efectos nocivos de la sociedad de control en el marco de los derechos humanos, consiguiendo una moderada habilitación del poder punitivo, con leyes penales sobre delitos informáticos, que son bien definidas y precisadas, con la mínima posibilidad de reducir espacios de libertad y de privacidad, e imponer penas considerando los datos del ser y la selectividad del poder punitivo, por consiguiente se reduce el estado de vulnerabilidad de todos los habitantes en especial de los más desfavorecidos, colaborando en realización del programa constitucional y el derecho internacional de los derechos humanos, mediante la prevención del genocidio por exacerbación del poder punitivo (Estado de Policía).

Fuente: Elaboración propia.

§ 2. OBJETO

1. El derecho penal informático humano, siguiendo al derecho penal humano, tiene dos objetos, el primero, es el objeto de estudio propiamente dicho, la seguridad jurídica de los delitos informáticos, y segundo, el objeto de interpretación.

2. La seguridad jurídica, la hereda del derecho penal, y ello importa asegurar la coexistencia de todos los humanos impidiendo el uso irracional de la fuerza que estallaría en una guerra civil, haciendo previsible las conductas de los demás respecto de los bienes jurídicos vinculados a las tecnologías de la información y la comunicación, asegurando la relación de disponibilidad de diversos entes necesarios para el desarrollo existencial en la que Mc Luhan llamaría la *aldea global* (1 993) que a nuestro entender

se encuentra controlada, en ese sentido, el derecho penal informático humano, desde un aspecto objetivo: Como lo enuncia Zaffaroni, cumple con la *función de proyectar la contención jurídica del poder punitivo y, por ende, la de proteger los bienes jurídicos, pero no los que el tipo objetivo exige que se ofendan, sino todos los bienes jurídicos, que dejarían de serlo en caso de quedar a merced del poder punitivo descontrolado*, y desde el aspecto subjetivo se mantiene el sentimiento de seguridad jurídica de niveles bajos de vulnerabilidad ante el ejercicio poder punitivo. (Zaffaroni, E. R., et al, 2 002, p. 80; 2 016; 1 998, p. 44-46; 2 012, p. 236).

3. El objeto, es tomado por la Doctrina como función o misión del Derecho Penal o es confundido con el objeto de interpretación (el derecho positivo) (Peña Cabrera Freyre, R., 2 015, p. 39; Kaufman, A., 2 013, p. 29; Polaino Navarrete, M., 2 008, p. 34) lo cual, a nuestro juicio, no es adecuado en la tarea de reconstruir el derecho penal con una dogmática deslegitimante, por cuanto se verá que la función o misión principal del derecho penal informático humano es la contención del poder punitivo.

4. El objeto principal de interpretación del derecho penal informático humano es la ley penal relativa a los delitos informáticos, considerando que la ley penal es fuente de conocimiento ineludible del derecho penal humano, siendo éste materia esencial para el estudio dogmático-jurídico en la tarea de la reducción del poder de vigilancia del poder punitivo en la sociedad de control. (Zaffaroni, et al, 2 011, p. 81, 88).

§ 3. FUNCIÓN

1. Tradicionalmente se suele equiparar la función del derecho penal a la función de la pena y la medida de seguridad (Mir Puig, S., 2 003, p. 48), el derecho penal humano de Zaffaroni, reclama una función autónoma, a la que se adscribe el derecho penal informático humano, y ésta es la función de contención o reducción del poder punitivo para fortalecer el Estado Constitucional de Derecho, que consiste en recortar la intensidad, extensión del poder de vigilancia del poder punitivo, o evitar los actos verticales de mayor irracionalidad en la sociedad de control, para ello se vale de las fuentes de conocimiento y de información del derecho penal, para orientar las decisiones de los operadores judiciales, mediante un sistema de comprensión que responde a un objetivo político, previamente establecido que es la contención del poder punitivo para preservar cuidadosamente los espacios de libertad que permitan el desarrollo de la dinámica, social y económica de nuestras sociedades (Zaffaroni, E. R., et al, 2 002, p. 96, 39; Zaffaroni, E. R., 2 016, 90).

2. La ideología de control asentada en la sociedad de control, se ha visto más predominante en la mayoría de Estados sobre todo en los autoritarios, que se han armado de equipos tecnológicos para vigilar sin medida a la población, en busca del enemigo, la cultura terrorista, ha motivado que las agencias de seguridad e inteligencia, se dediquen a recopilar datos de Internet, para analizarlos y alimentar bases de datos de potenciales enemigos (terroristas, activistas de derechos humanos, periodistas, políticos, etc.), ello ha obligado a que los ciudadanos ingresen a un submundo digital, llamado Darknet, navegando de forma anónima, en medio de verdaderos delincuentes (vendedores de drogas, armas, sicarios, etc.) (DW, 2 017, May, 25), V.gr. El espionaje cibernético de Irán a exiliados o disidentes ubicado en otros países, siendo difícil

atribuir los ataques con Malware al Gobierno como en la India o Vietnam, o el espionaje del Gobierno mexicano a activistas y periodistas (Insider.pro, 2 016; Guarnieri, Schosser, 2 013; Ahmed, A. y Perlroth, N., 2 017, June 19.); al respecto Marek Marczynski, Director de asuntos militares, de seguridad y policiales de Amnistía Internacional, señala que los Gobiernos recurren cada vez más a tecnología peligrosa y sofisticada que les permite leer correo privado de activistas y periodistas y activar a distancia la cámara o el micrófono de sus ordenadores para registrar clandestinamente sus actividades. Usan la tecnología en un cobarde intento de impedir que los abusos salgan a la luz (Amnistía Internacional, 2 014), y hasta el país más democrático -en apariencia- están del lado del control pernicioso, lo notamos con WikiLeaks, que reveló que la CIA tiene un sistema -llamado proyecto Dumbo- que puede eliminar o manipular archivos de video, y controlar las cámaras web y los micrófonos de los ordenadores con Microsoft Windows. (RT, 2 017, August 3).

3. De otro lado, la criminalidad informática, está golpeando los sistemas informáticos de manera global, como los ataques de tipo ransomware del 12 de mayo y 27 de junio de 2 017, que afectó a 150 países de Europa, América Latina y Asia, secuestrando archivos a cambio de Bitcoins, para liberar los sistemas hospitalarios, de telefonía, ordenadores de los Ministerios del Interior y Salud de Rusia, laboratorios de Universidades, planta nuclear de Chernóbil que estuvieron paralizados a causa de los virus informáticos WannaCry y Petwrap, que según Snowden y Vince Steckler, Director Ejecutivo de la Compañía de Seguridad Informática Avast, se trataría de un arma secreta de la NSA que fue filtrada. (Cf. DW, 2 017, May, 12; Infobae, 2 017, May, 12; RT, 2 017, May, 15; RT, 2 017, May, 12; BBC Mundo, 2 017, June 27).

4. El poder punitivo se habilitó para el efectivo control de las Tecnologías de la Información y de la Comunicación (TIC), mediante las leyes penales de delitos informáticos, amplificando el poder de vigilancia de la sociedad de control, en el marco de la llamada Tercera Guerra Mundial no declarada que a decir del jurista argentino Zaffaroni, fomenta la conflictividad entre los más pobres como parte de una tarea genocida por goteo, al tiempo que obstaculiza la concientización, la coalición y el protagonismo político coherente y organizado de los excluidos (2 015, p. 203-204).

5. En esta guerra no declarada, las TIC, son instrumentos de espionaje y armas de ataque para Gobiernos y terroristas, y un medio para construir zonas oscuras de clandestinidad para el delincuente y para el ciudadano paranoico, hostigado por la persecución política, mientras que para el resto de usuarios entre jóvenes y adultos con Smartphone, las TIC, significa entretenimiento, social media, noticias, portales, servicios, juegos, estilos de vida, deportes, familia y juventud, y retail, (ComScore, 2 016 y 2 015); con la criminalización secundaria (selectividad), son los más débiles y desfavorecidos quienes, con los tipos penales de delitos informáticos, incrementa su vulnerabilidad frente al poder punitivo, por cuanto en una guerra global somos todos los civiles de cualquier país, quienes nos encontramos indefensos frente a los agentes ejecutivos, quienes podrían confundirnos con terroristas o delincuentes que penetran sistemas informáticos, digamos que tener smartphone equivaldría a poseer un arma blanca, y una laptop con navegador Tor (deep web para evitar el poder de vigilancia) o software de programación a llevar consigo un arma de fuego, es decir un potencial delincuente en actos preparatorios de algún imaginado plan criminal.

6. La selectividad del poder punitivo y la irracionalidad con la que actúan los agentes ejecutivos (policías), obligan al derecho penal informático a contener o reducir al poder punitivo, sobre todo a ese poder de vigilancia, preservando los pequeños espacios libertad y privacidad que aún contamos, mediante la dogmática deslegitimante del poder jurídico que, parafraseando a Zaffaroni, actúa como un semáforo verde para los jueces, para dejar pasar el poder punitivo, ámbar para detenernos a pensar, y rojo para detener el poder punitivo, a efectos de evitar la instalación de un Estado de Policía, convirtiendo a los delitos informáticos en un verdadero panóptico del poder punitivo. (Espinoza Coila, M., 2 014).

§ 4. CARACTERES

1. Siendo el derecho penal informático humano, parte del derecho penal humano, asume sus caracteres, siendo los siguientes: a) *Público*, porque es una parte del derecho penal humano que pertenece al derecho público. b) *Represivo*, porque el poder punitivo necesita represión para posibilitar la civilización. El derecho penal informático humano debe operar como dique para represar las pulsiones irracionales del poder punitivo del Estado en la sociedad de control; c) *Continuo y fragmentador*, porque el derecho penal informático humano, se debe mantener siempre atento para identificar al poder punitivo a fin de contener su estructural tendencia a la continuidad que sin la contención desembocaría en el Estado Totalitario y fragmentarlo o acentuarlo según el poder jurídico que ejercen las agencias judiciales; d) *Normativo*, porque el derecho penal informático humano se ocupa de las leyes penales sobre delitos informáticos, de ellas se infieren normas deducidas, que cumplen una función dialéctica, en el plano político, habilita la criminalización secundaria, y en el plano jurídico, sirve para limitar al poder punitivo. (Zaffaroni, E. R., et al, 2 002, p. 96-97; 2 011, p.79-83).

2. En la Doctrina, también se mencionan otras características que se le atribuyen al Derecho Penal, por una confusión con la ley penal: a) *Sancionatoria*, el que es sancionador es la ley penal como sostiene Zaffaroni, b) *Personalismo*, porque el destinatario de la ley penal es el delincuente a quien le corresponde la sanción, c) *Valorativo*, por los juicios de valor sobre los hechos o conductas humanas que están previstos en la ley penal, d) *Finalista*, porque la ley penal persigue protección de los bienes jurídicos de relevancia penal, el derecho penal informático humano, en cuanto saber penal, sería también *finalista*, cuando busca la reducción del poder punitivo en la sociedad de control. (Peña Cabrera, R., 1 986, p.24-25; Creus, C., 1 992, p. 4; Fontan Balestra, C., 1 998, p.23).

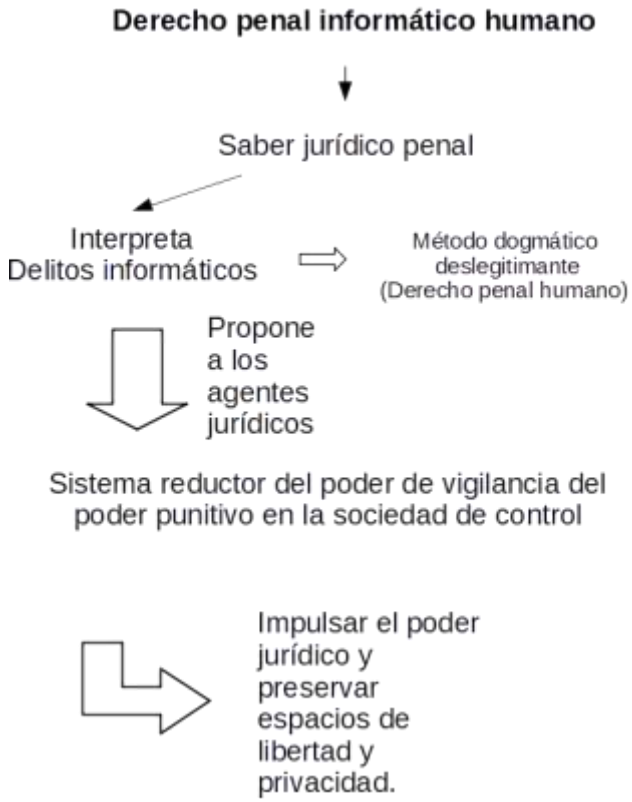

Figura 1. Diagrama de los límites u horizonte de proyección del derecho penal informático, con el cual se representa la definición que proponemos, sobre la base del derecho penal humano.Fuente: Elaboración propia.

4.2. LA NECESARIA INTERDICIPLINARIEDAD SECANTE ENTRE EL DERECHO INFORMÁTICO Y EL DERECHO PENAL

§ 1. DERECHO INFORMÁTICO

1. La informatización de la sociedad, por la influencia de las Tecnologías de la Información y Comunicación –TIC- en lo jurídico, han insuflado fenómenos teóricos interdisciplinarios en el Derecho, como el «Derecho Informático», que es una rama de las Ciencias Jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática); de este modo, el derecho ha pretendido regular la informática, mediante (a) el empleo de la computadora en el ámbito jurídico, o, (b) como leyes, normas, principios aplicables a los hechos y actos derivados de la informática. (Téllez Valdés, J. A., 2 008, p. 9-10, 13).

2. El jurista Julio Téllez Valdés, sostiene que a) *La informática jurídica,* es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como a la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación, verbigracia, los software de tratamiento y gestión de leyes, jurisprudencia y doctrina como LexisNexis, Vlex, Sistema Peruano de Información Jurídica. (SPIJ); o sistemas expertos como los sistemas de apoyo a la gestión fiscal o jurisdiccional; y b) Sobre el *derecho de la informática,* es un conjunto de leyes (ordenamientos jurídicos nacionales e internacionales) que se ocupan de los fenómenos informáticos, normas en virtud de aquellas que integran la llamada *Política Informática*, principios en función de aquellos postulados emitidos por jueces, magistrados, tratadistas y estudiosos respecto al terna, por otra parte el jurista mexicano, se refiere a hechos como resultado de un fenómeno aparejado a la

informática inimputable al hombre, y actos como resultado de un fenómeno directamente vinculado con la informática y provocado por el hombre.

3. Con el tránsito de la comunicación oral, escrita (Gutemberg) y digital (la computadora u ordenador), la comunidad humana ha conseguido un relativo desarrollo, en ese sentido la ciencia del derecho, no ha sido ajeno en considerar a las computadoras como elementos básicos de la vida dentro del proceso evolutivo en el manejo, posesión y distribución de la información que está directamente relacionado con el poder, la prosperidad, la democracia, el desarrollo económico y el avance de la ciencia. (Sartori, G., 2 004; Arata Salinas, A.A., 2 002, p. 25), por ello cobra sentido la visión interdisciplinaria entre el Derecho y la Informática, que permite al legislador establece reglas, que pretenden tratar la problemática actual de los delitos informáticos, la propiedad intelectual, regulación de la información, del Internet, contratos informáticos, comercio electrónico, spam, documentos electrónicos, informática forense, teletrabajo y otros aspectos vinculados a la informática.

§ 2. DERECHO PENAL

1. El *Derecho Penal*, es la rama del saber jurídico que, mediante la interpretación de las leyes penales, propone a los jueces un sistema orientador de decisiones que contiene y reduce el poder punitivo, para impulsar el progreso del Estado Constitucional de Derecho. (Zaffaroni, E. R., 2 002, p, 5).

2. El *Poder Punitivo*, es el que ejerce (o deja ejercer) el Estado, cuando no tiene por objeto reparar un daño o detener un proceso lesivo en curso o inminente, es decir, cuando no entra en el esquema reparador del derecho privado o en la coerción directa del derecho administrativo. (Zaffaroni, E. R., 2 016).

3. Cuando hablamos de Derecho Penal, nos referimos al derecho penal humano, propuesta teórica del profesor Raúl Zaffaroni, surgida por la necesidad de repensar el derecho penal para la prevención del genocidio, según el cual el *operador jurídico*:

> (…) está forzado a ser siempre contrapulsionador de fuerzas irracionales, debiendo valorar en cada caso el grado de irracionalidad del poder punitivo que le incumbe filtrar, con el objeto de evitar el paso de sus manifestaciones más irracionales, pero sin pretender demarcaciones estáticas e invariables, puesto que su actividad confrontativa es por esencia incompatible con señalizaciones de esa naturaleza. En este sentido, la empresa del derecho penal humano es un *unfinished*. (2 016).

4. En consecuencia, el derecho penal, contrapulsiona las irracionalidades del poder punitivo y bien puede ocuparse de las leyes penales manifiestas sobre delitos informáticos.

§ 3. LA CORRESPONDENCIA ENTRE SABERES JURÍDICOS

1. El *Derecho Penal Informático* es producto del binomio derecho informático - derecho penal, descritos por el principio de interacción, en donde existe una relación recíproca por el aporte de sus conocimientos para resolver los problemas actuales relativos al tratamiento de las Tecnologías de la Información y la Comunicación en el Derecho Penal, de este modo, el Derecho Informático se presenta como una glosa de las cuestiones tecnológicas para el derecho penal, y el derecho penal actúa como un sistema de comprensión de los delitos informáticos que permite al derecho informático escrutar el poder punitivo en la sociedad de control.

2. La correspondencia entre los descritos saberes jurídicos es de forma secante por la superposición en sus horizontes de proyección para la adecuada interpretación de los delitos informáticos, la sinergia de ambos saberes jurídicos permiten garantizar el *nullum crimen sine conducta,* para ello es menester el trabajo conjunto y necesario del derecho penal con sus principios constructivos y su dogmática deslegitimante, y del derecho informático que se encarga de la comprensión de los fenómenos informáticos; la sinergia de ambos saberes optimiza la reducción del poder de vigilancia del poder punitivo en la sociedad de control, que pretende consolidar el panóptico del poder punitivo, el cual se describe como una sociedad totalitaria donde unos cuantos dirigen y se apropian de la información privada obtenida por una supervigilancia a cada habitante del planeta, quienes son más vulnerables a la coerción estatal no reparadora ni interruptora de procesos lesivos inminentes, por ser el nuevo enemigo de los Estados verticalizantes . (Espinoza Coila, M., 2 015).

3. La eclosión de la informática y el uso masivo de las Tecnologías de la Información y la Comunicación, han originado nuevas formas de criminalidad y el anonimato como contenido del derecho a la privacidad nos conducen a una tensión entre los avances tecnológicos y el derecho penal, situación que ha permitido al poder punitivo crear un nuevo enemigo: el ciberterrorista, un enemigo del Estado armado de equipos informáticos de intrusión, espionaje, y sabotaje de sistemas informáticos, un típico ciberdelincuente llamado *hacker o cracker*; de otro lado la cultura del terrorismo se manifiesta en los medios para alimentar un discurso legitimante del poder punitivo, esto es, el discurso del ciberterrorismo, como consecuencia del desarrollo de la sociedad de la información que ha generado una criminalidad compleja que sitúa al Derecho Penal frente a nuevos retos categoriales (Sieber, U., 2 008, p. 127, 133; RT, 2 014, December 22).

4. Es sumamente importante el intercambio de datos del Derecho Penal y el Derecho Informático, pues ello permite edificar un saber interdisciplinario para el tratamiento de los delitos informáticos en el marco de la criminalidad compleja, y como afirma el profesor Raúl Zaffaroni:

> (...) La doctrina penal debe reconocer diversos fenómenos del poder punitivo real en nuestra sociedad, sea para contenerlos, tratar de desbaratarlos o tener en cuenta sus efectos, so pena de formar una doctrina enferma, que alucine un mundo no real y proyecte decisiones para ese mundo inexistente. (2 015, p. 230).

5. La construcción de un derecho penal informático, para que sea humano e integral debe comprender todos los fenómenos tecnológicos, políticos, económicos ligados a los delitos informáticos, ello porque el derecho penal no es un saber monolítico; sino que es un proyecto de jurisprudencia tejido con hilos provenientes de una interdisciplinariedad secante y tangente con saberes jurídicos y no jurídicos, cuya proyección en el sistema judicial permite al poder jurídico contar con una herramienta de contención del poder punitivo, por ende evitar genocidios.

6. Consideramos que el *Derecho Informático,* es una fuente de conocimiento de primer orden para el saber penal, pues se trata de una condición *sine qua non* para la construcción del derecho penal informático, que incorpora datos técnicos legales de la informática (informatique) que se ocupa del tratamiento automatizado de los datos contenidos en los documentos, ello implica operaciones relacionadas a la toma de datos, almacenamiento, análisis documental, recuperación de información, transmisión de datos, reproducción de documentos y control documental (Curras Puente, E., 1 988, p. 217; Chiara Galván, E. R., p. 25), de igual manera el derecho penal humano, que nos

ofrece la dogmática deslegitimante como método para la reducción del poder de vigilancia, todo esto puede apreciarse en la Figura 2.

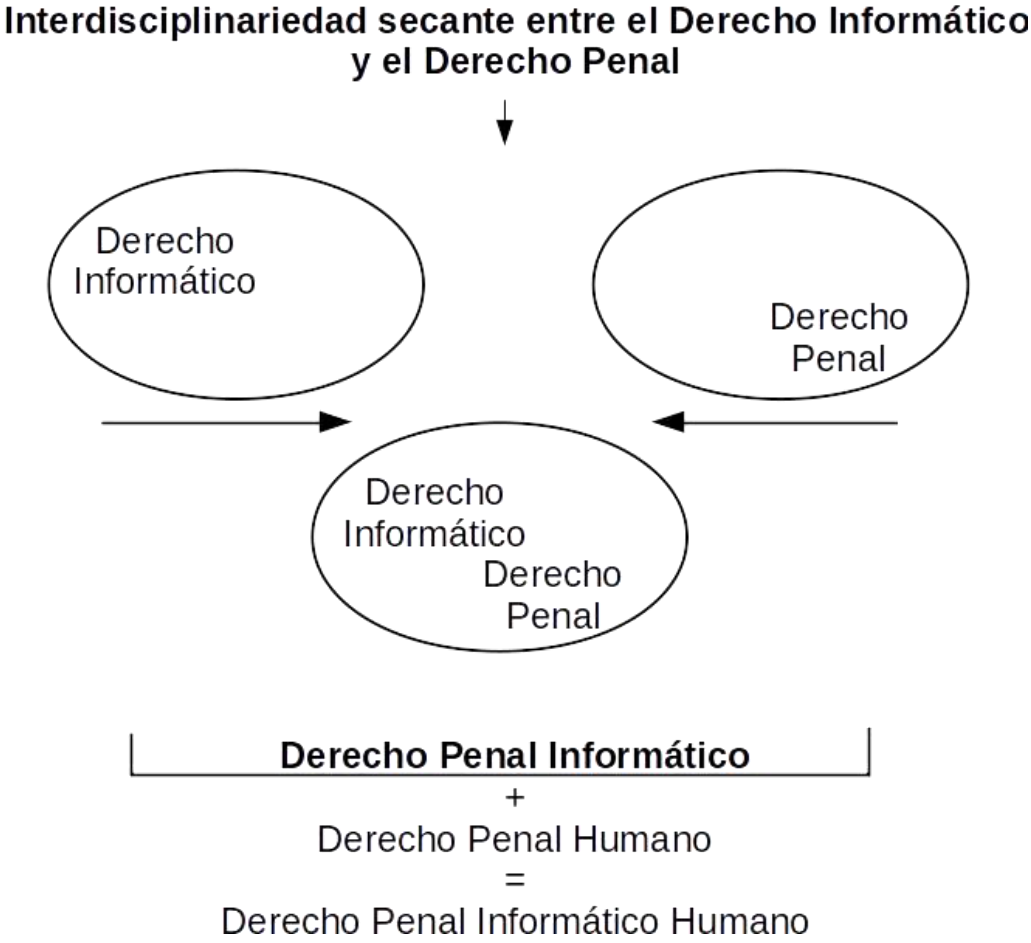

Figura 2. Diagrama de la interdisciplinariedad secante entre el Derecho Informático y el Derecho Penal, y la adición con el Derecho Penal Humano, del cual resulta el Derecho Penal Informático Humano. Fuente: Elaboración propia.

4.3. FUENTES DEL DERECHO PENAL INFORMÁTICO HUMANO

§ 1. DEL SABER PENAL

1. Siguiendo al derecho penal humano, el derecho penal informático, como saber jurídico penal, tiene dos Fuentes: *a) Conocimiento,* que comprende a todas las leyes sobre delitos informáticos que habilitan el ejercicio del poder punitivo (incluye a las inconstitucionales), y otros datos aportados por la interdisciplinariedad con el Derecho Constitucional, internacional, informático, administrativo, civil, jurisprudencia, filosofía, historia, política, economía y otros datos de la realidad, para aclarar el efecto real de las normas en el sistema penal, su funcionamiento y críticas ideológicas; y *b) Información,* que está compuesta por la bibliografía jurídico-penal sobre delitos informáticos que permite conocer el estado de desarrollo del derecho penal informático. (Zaffaroni, E. R. et al, 2 002, p. 102-106).

2. Sin las Fuentes de Conocimiento y Producción, el derecho penal informático estaría desprovisto de los datos necesarios para plantear soluciones normativas para reducir al poder punitivo, y su horizonte de proyección se vería limitado solo al tipo normativo, imposibilitado de compararla con otras normas y datos que revelen sus efectos potenciadores del poder de vigilancia del poder punitivo, y sería incapaz de responder al por qué y el para qué de la actuación estatal en la criminalización de las Tecnologías de la Información y la Comunicación, dado que el sistema propuesto actuaría como un miope, siendo menester apoyarse en otros datos para superar la oscuridad de la caverna y salir hacia la luz de la realidad objetiva.

§ 2. LA HISTORIA COMO FUENTE DE CONOCIMIENTO DEL DERECHO PENAL INFORMÁTICO

1. Los datos históricos, también son importantes para el derecho penal informático, puesto que nos ayuda a develar las manifestaciones del poder de vigilancia del poder punitivo en las sociedades humanas, dado que el objeto legítimo del conocimiento histórico -como señala R. Gray quien es citado por Silva Santiesteban, F. (1 983, p. 9)- es ayudar a la gente a comprender su situación haciéndole inteligible el pasado; accediendo al pasado, observaremos cómo se forjó la Sociedad de Control.

2. En efecto, la Historia nos permite comprender que el ser humano, desde sus primeros pasos, se propuso facilitar su actuar perfeccionando progresivamente sus métodos, sus técnicas e instrumentos de manejo de información mediante representaciones pictográficas en piedra, edificaciones (estatuas, templos), herramientas de conteo como el quipu, y otras invenciones de procesamiento de información, desde los más rudimentarios, desde el ábaco hasta los enormes bancos de datos o *data center* gestionados por ordenadores (informática), accedidos de forma remota o consultados vía Web con un teléfono móvil (telemática). En 1 983 Frosini, divide en cuatro etapas la evolución de la informática, la *primera* es la comunicación puramente oral, la *segunda*, los símbolos y la forma escrita del lenguaje, la *tercera*, la reproducción de mensajes con la invención de la imprenta y la *cuarta*, con la aparición de la computadora y las redes de información (p. 45-46), de otro lado, el poder punitivo siempre estuvo presente en el control de la producción de la información, a través de la ética y deontología en sus inicios, posteriormente con normas sobre publicación de obras (Roma, Partidas de Alfonso X), la preocupación por la autoría con el Estatuto de la Reina Ana de Inglaterra (1 710) y la Convención de Berna (1 886), por ello, el derecho penal informático

entorno a la historia, debe efectuar una genealogía de los tipos penales sobre delitos informáticos, que se refiere a proceder a rastrearlos a través de códigos y leyes de diferentes épocas (Zaffaroni, E. R., 2 009b, p.13-14), para hacerlos -en palabras de Foucault-, capaces de oposición y de lucha contra la coerción de un discurso teórico, unitario, formal y científico (1 998, p. 20).

3. La genealogía no se conforma con el análisis temporal; sino que se proyecta al espacio, con el *Derecho Comparado* (*Rechtsgleichung*), que connota un proceso de comparación, libre de cualquier implicación de la existencia de un cuerpo de normas que formen una rama distinta o un área específica del Derecho (Gutteridge, H. C., 1 946, p.1), con lo cual, se puede realizar una investigación histórico-comparativa del tipo penal en cuestión, en razón que, parafraseando al maestro Zaffaroni, la formulación legal es construida por un legislador histórico en un momento y lugar dados, en un contexto de poder, en la que el legislador imaginó que decidía un conflicto en favor de los intereses de cierto grupo o sector social. (2 009b, p. 15, 17).

§ 4. DE LA LEGISLACIÓN PENAL

1. El derecho penal informático, como legislación penal, tiene dos Fuentes: *a) Conocimiento*, que comprende a las leyes penales constitucionales (lícitas) sobre delitos informáticos, que por lo menos gocen de la presunción de constitucionalidad; y *b) Producción*, son las instituciones u órganos constitucionalmente habilitadas para la sanción de leyes penales, como el Congreso o Parlamento, o el órgano de función ejecutiva previa delegación por el Legislativo.

2. El profesor Zaffaroni, indica que en la tarea de contención del poder punitivo, hay tres momentos en el conocimiento de la ley penal: 1) Precisar las leyes penales constitucionales lícitas y autoridad conforme al procedimiento constitucional, 2) Conocer todas las leyes penales constitucionales o inconstitucionales que programen, habiliten o posibiliten el ejercicio de algún poder punitivo (leyes, decretos, ordenanzas municipales, resoluciones ministeriales, etc.) y las respectivas autoridades de que emanan, y 3) Comparar el tipo normativo de la legislación penal constitucional con la legislación vigente que habilita o posibilita el ejercicio del poder punitivo, para programar la declaración de inconstitucionalidad de la que no resulta adecuada al tipo normativo de leyes penales formalmente constitucionales, se trata de una elaboración dialéctica reductora del poder punitivo (Zaffaroni, E. R. et al, 2 002, p. 101-102).

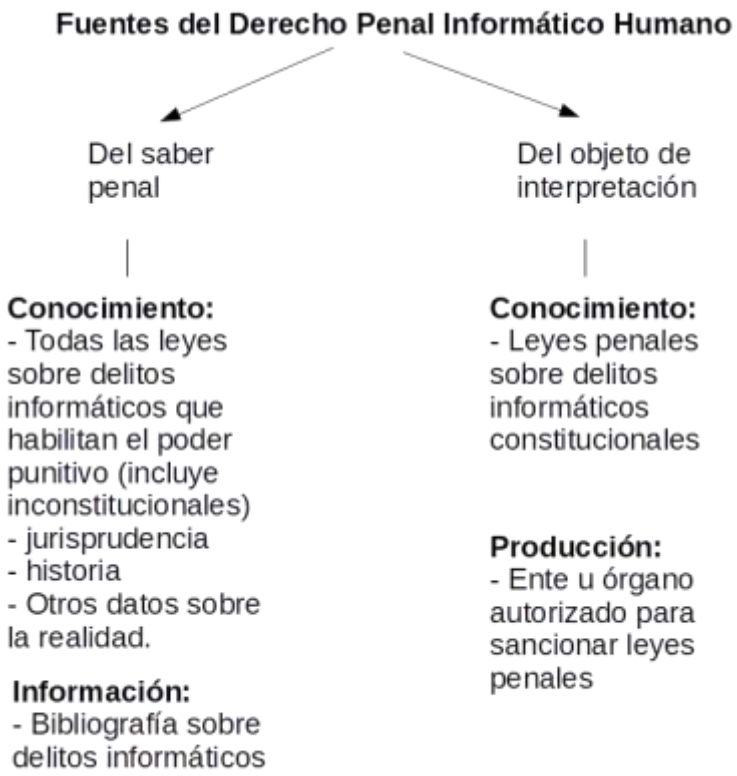

Figura 3. Diagrama que presenta a las Fuentes del Derecho Penal Informático Humano, del que se distinguen, el saber penal (programa de jurisprudencia del derecho penal) y el

objeto de interpretación (legislación penal sobre delitos informáticos) Fuente: Elaboración propia.

4.4. EL DELITO INFORMÁTICO

§ 1. DEFINICIÓN

1. El *Delito Informático* (computer crime / computerkriminalität), es definido de manera *(a) formal*, como acción u omisión prohibida por la ley penal sobre delitos informáticos; *(b) material*, como conducta final que ofenden bienes jurídicos relacionados a las Tecnologías de la Información y la Comunicación, y *(c) analítica*, como conducta típica, antijurídica y culpable que tiene como medio u objeto de protección a las Tecnologías de la Información y Comunicación. (Espinoza Coila, M., 2 014, p. 14).

2. Entre todas las definiciones, la *analítica* nos parece más fecunda, porque nos indica cuáles son los elementos mínimos que deben acreditarse con la Teoría del Delito para emitir una sentencia condenatoria que da luz verde en el semáforo del poder jurídico, esto es, que permite avanzar al poder punitivo con la pena sobre el condenado.

3. La doctrina ofrece otras definiciones y distinciones al tratar la definición de los *Delitos Informáticos*, así tenemos a los siguientes autores: *(a)* Julio Téllez, para quien son actitudes ilícitas que tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin (concepto típico) (2 008, p. 188); *(b)* Santiago Acurio, quien luego de analizar los trabajos de Nidia Callegari, Miguel Davara, Donn

Parker, María Castillo y Miguel Ramallo, Marcelo Huerta y Claudio Líbano, concluye que la *delincuencia informática*, es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera. (2 007, p. 14);*(c)* Andrés Campoli, quien sostiene que los *delitos informáticos*, son aquellos en los cuales el tipo penal protege la integridad física o lógica de los equipos informáticos o páginas web (hacking, cracking), y prefiere definir a los *Delitos Telemáticos*, que son aquellos que, sin afectar expresamente a un equipo informático en particular disminuyen o anulan su capacidad de transmisión o procedimiento de datos a distancia, ya sea actuando en forma indirecta sobre el equipo, sobre su capacidad de receptación o envió de datos, sobre sus parámetros lógicos o sobre las vías de comunicación necesarias para las funciones normales del mismo, a distancia (phreaking, interceptación de datos) (2 013, p. 35); *(d)* María Viega, opina que los *Delitos Informáticos*, se pueden definir como toda conducta ilícita, sancionada por el derecho penal, para la realización de la cual se utilizan los medios informáticos, frutos de las nuevas tecnologías, ya sea como herramienta para la comisión del delito o como fin en sí mismo, afectando los datos contenidos en un sistema. (n.d.); *(e)* Felipe Villavicencio, entiende por *Criminalidad Informática*, como aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidos a través de la Tecnología. (2 015); *(f)* Luis Bramont-Arias Torres, define el *delito informático*, como aquél en el que, para su comisión, se emplea un sistema automático de procesamiento de datos o de transmisión de datos. (2 000); *(g)* Juan Blossiers y Sylvia B. Calderón, afirman que el *Delito Informático*, es toda acción consciente y voluntaria que provoca

un perjuicio a persona natural o jurídica sin que necesariamente conlleve a un beneficio material para su autor, o que por el contrario produce un beneficio ilícito para su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión interviene indispensablemente de forma activa dispositivos normalmente utilizados en las actividades informáticas. (n.d.); *(h)* Julio Núñez, define a los *Delitos Informáticos*, son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático. (1 999); *(i)* Luis Reyna Alfaro, prefiere distinguir entre *Delitos Computacionales*, que son aquellos para cuya comisión el autor se ha valido de un medio informático, diferenciándolo de los *Delitos Informáticos*, que son aquellas conductas que afectan a un nuevo interés social, íntimamente ligado al tratamiento de la información, en la misma línea el jurista Juan José Gonzales Rus, diferencia entre objeto material del delito y medio de comisión del delito, el primero alude al Hardware y Software que son protegidos, y el segundo se refiere a los sistemas o elementos informáticos que son instrumentos para la realización de delitos. (2 002, p. 167, 133, 135); *(j)* Ulrich Sieber, prefiere adherirse a la definición de la OCDE (Organización para la Cooperación y el Desarrollo Económicos), que define al *Delito Informático* o *Crimen Informático*, como cualquier ilegal, antiético, o comportamiento no autorizado que implica la automatización de datos, procesamiento y/o transmisión de datos. (1 998, p. 19); *(k)* Klaus Tiedemann, prefiere la expresión "criminalidad mediante computadoras", que alude a todos los comportamientos antijurídicos según la ley vigente (o socialmente perjudiciales y por eso punibles en el futuro) realizados merced al empleo de un equipo automático de procesamiento de datos. (1 985), etcétera.

4. El estudio de los delitos informáticos o la criminalidad informática, nace en medio de la guerra fría, caracterizada por el desarrollo electrónico y la automatización promovida por la competición entre la URSS y los Estados Unidos, cuyas conquistas tecnológicas, dejaron como legado el ordenador o computadora y la Arpanet (actual Internet). (Pirenne, J, 1 980, p. 497-509; Infobae, 2 004, September 13), la preocupación por su naturaleza y tipología, y sus implicancias legales en el mundo, emergió de organizaciones internacionales que intentan ofrecer una visión global de los delitos informáticos, tales como la Unión Internacional de Telecomunicaciones (ITU), la INTERPOL, la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), G8, el Consejo de Europa, Organización de Estados Americanos (OEA), Foro de Cooperación Económica Asia-Pacífico (APEC), la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el Commonwealth, Unión Europea, las Naciones Unidas, OTAN, OEA y otras organizaciones internacionales, que han realizado esfuerzos para asegurar la armonización de las legislaciones de los países del globo. (Schjolberg, S, 2 008), quizá el avance más grande se dio con el Convenio del Consejo de Europa sobre la ciberdelincuencia, conocida como la Convención de Budapest, emitido en Hungría, el 23 de noviembre del 2 001, y que entró en vigor el 01 de julio del 2 004, y con éste, impulsó el tratamiento de los ataques contras las Tecnologías de la Información y Comunicación, se perfiló como asunto de agenda mundial.

5. No obstante, la gran preocupación mundial por el crimen informático, aún el delito informático no tiene una definición unánime, solo sabemos que todas presentan en común, conductas asociadas a las Tecnologías de la Información y Comunicación,

esto no precisa nada, por ello creemos que éstas deben declarar expresamente los requisitos de operatividad para acotar el poder punitivo.

§ 2. FUNCIÓN

1. Los delitos informáticos, tomando como base la bifrontalidad del tipo (núcleo duro del delito) (Zaffaroni, E. R.; et al, 2 011, p. 340), asumen una doble función en la sociedad de control: a) Habilitar el ejercicio del poder punitivo, y a la vez b) Limitar al poder punitivo mediante la interpretación del tipo con una dogmática deslegitimante y estableciendo los caracteres propios del delito que han de acreditarse para dejar pasar las aguas menos turbias o intensas del poder punitivo.

2. La doble funcionalidad, se trata de una dialéctica siempre presente en la contención del poder de vigilancia del poder punitivo, se puede ejemplificar con un grifo de agua, el legislador imagina resolver algo y sanciona un delito, el policía y el fiscal u otro agente ejecutivo especializado en delitos informáticos o de alta tecnología, intervienen en flagrancia o promueven una investigación contra un ciudadano estereotipado, abriendo un poco el grifo del poder punitivo que tiende siempre a potenciar la vigilancia que siempre está presente en mayor o menor medida en la llamada *Sociedad de Control* sobre la vida digital, ante ello, el mismo tipo que incremento de la situación de vulnerabilidad del investigado, señala el ámbito de prohibición al juez quien tiene la potestad de cerrar definitivamente o abrir más el grifo de agua, dejando que caiga el agua sobre el imputado, cabe aclarar solo controla el grifo mas no puede dominar el flujo de agua que circula en las cañerías que forma parte del sistema de abastecimiento de agua, el poder punitivo siempre estará presente y listo para salir por el grifo, el poder jurídico, no puede detenerlo plenamente, como diría el

maestro Zaffaroni, solo se puede filtrar las aguas más irracionales hasta nivelarlo mediante la teoría del delito que opera como un dique de contención de las aguas más turbulentas. (2 002, p. 373).

3. De otro lado, en la Doctrina hay otras funciones, como la de garantía enunciada por Beling, quien sostiene que desde el punto de vista jurídico - político, no puede incoarse un proceso penal y una condena, sin tomar como base el delito objeto del proceso y notificado a la parte interesada, cuya defensa se elaboró en función del hecho típico planteado en la acusación (2 002, p. 310), aunque esta función nos conduce al problema de los tipos abiertos, pues como señala Roxin, éstos no cumplen con dicha función. (2 014, p. 179), esta cuestión de legalidad también presente con los tipos de peligro, se ven superados, como señala el profesor Zaffaroni, con el mismo Derecho Penal que es el encargado de completarla y traducirla en términos de legalidad estricta, mediante interpretación limitativa o con la inconstitucionalidad. (2 002, p. 441), esto por exigencia del Principio de Legalidad, que a propósito Beccaria, nos diría "Haced que las leyes sean claras y simples (...)", incluso, a su modo de ver la observancia a este precepto evitarían delitos. (1 993, p. 159).

§ 3. CARACTERÍSTICAS

1. Con relación a las características de los delitos informáticos o delitos cibernéticos, en la Doctrina (Téllez Valdés, J., 2 008, p. 188-189; Acosta Patroni, A. p. 31-40), se menciona que son: *(1)* Conductas criminales de cuello blanco, porque sólo determinado número de personas con ciertos conocimientos técnicos pueden cometerlas, cuestión que será mejor analizada en la § 5(sujetos); *(2)* Acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando; *(3)* Acciones de

oportunidad, porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico; *(4)* Provocadoras de serias pérdidas económicas; *(5)* Se realizan con facilidad de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física, *(6)* Difícil averiguación y comprobación, porque sus autores actúan de forma anónima valiéndose de servidores proxys, servidores de email anónimos, direcciones ip dinámicas, conectado por wifi, son usuarios de cabinas de Internet, también operan en la DarkNet, como Onion (un espacio de Internet donde se puede navegar de forma anónima), de este modo, las cifras negras de usuarios y de delitos es incierta, lo único que sabemos es de la existencia de los bitcoins; *(7)* Sofisticados y relativamente frecuentes en el ámbito militar, por lo que, *(8)* Presentan grandes dificultades para su comprobación, por su carácter técnico; *(9)* En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales; *(10)* Ofrecen a los menores de edad facilidades para su comisión, *(11)* Tienden a proliferarse cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional; *(12) D*e mera actividad y con permanencia del hecho, pueden repetirse continuamente en el tiempo, en razón que son de comisión instantánea, se perfeccionan con la acción u omisión, no es necesario el daño, sus efectos son permanentes; además que son, *(13)* Pluriofensivos y masivos, porque pueden afectar varios bienes jurídicos y a varios sujetos pasivos; y *(14)* Transfronterizos, porque se valen del Internet, por lo que puede tener efectos en varios países.

2. Podemos ejemplificar a los delitos informáticos con los casos expuestos por la Oficina de las Naciones Unidas contra la Droga y el Delito (2 012, p. 121):

Caso HUN 1: Los dos principales organizadores de un grupo de aproximadamente 30 personas prestaban actividades como servidores legales, alojando servicios para varias personas y asociaciones comerciales privadas. A través de esta actividad, enmascararon cientos de "smswarez"- (es expresión que en la jerga de Internet indica el comercio ilegal de contenidos protegidos por derechos de autor a cambio de un pago a través de SMS), "smswebs" (página a partir de la cual pueden descargarse contenidos protegidos por derechos de autor a cambio de sms-es) y "torrents" (sistema en el cual un usuario de Internet descarga el archivo, o partes del archivo deseado, no desde un servidor central; sino desde otros usuarios desconocidos, que ya lo tienen). La ventaja de este último sistema es que, si un archivo se hace muy popular, aún más personas participan en la descarga y de esta forma la distribución se hace más efectiva. Los servicios ilícitos se anunciaban con sus accesorios en forma de spams. Se incautaron 48 servidores ilegales con un tamaño de 200-250 terabytes y otros suministros de alta tecnología en 16 instalaciones diferentes. El experto evalúa que "se ha liquidado una organización delincuencial basada en Internet, con relaciones profesionales a todo lo largo del país. La gravedad de la actividad ilegal quedó confirmada por el hecho de que, según la información disponible, el volumen de los datos ilegales confiscados alrededor del mundo llega a los 45 terabytes. Luego de esta acción, el movimiento de datos por Internet se ha reducido (10%) en todo el país".

Caso RUS 13: Éste es un caso de extorsión a una escala particularmente grande, cuyas víctimas principales fueron corredores de apuestas británicos. Funcionarios de la Unidad Nacional del Reino Unido contra Delitos de Alta Tecnología (NHTCU, más tarde, Agencia para el Delito Organizado Grave -

SOCA) y el Servicio Secreto de los Estados Unidos estuvieron directamente involucrados en la investigación. El grupo delictivo decidió utilizar una red de computadoras a la que tenían acceso y que habían infectado con malware especialmente escrito (programas DdoS) sin el conocimiento de los propietarios. Desde esas computadoras podían lanzar ataques distribuidos sin el conocimiento del usuario, que causarían negaciones de servicio distribuidas (DDoS). Los papeles asignados a los miembros de la organización delincuencial implicaban todos conocimiento y habilidades cibernéticas especializadas: Por ejemplo, cómo preparar un módulo de programa especial que corra programas auto replicantes y explote debilidades en el Sistema Operativo Windows, para obtener el control de computadoras remotas sin conocimiento del usuario; cómo monitorear un ataque mientras golpea los servidores y remediar fallas o mal funcionamiento; cómo estudiar nuevos virus de computadora para su uso posterior por parte del grupo. Para enmascarar sus actividades delincuenciales, utilizaban, entre otros, servidores proxy anónimos, servicios de red privada virtual (VPN) y servidores de correo anónimos. El dinero extorsionado fue enviado, a través de redes internacionales de pago existentes, a personas residentes en Letonia, quienes hicieron los arreglos para su transferencia a Rusia. Las víctimas de la extorsión fueron compañías corredoras de apuestas, cuyo negocio depende enteramente del acceso a Internet, ya que las apuestas se hacían exclusivamente vía Internet. Por ejemplo, un ataque inundó el servidor de la compañía objetivo con aproximadamente 425 direcciones IP únicas que establecieron más de 600 000 conexiones simultáneas con el servidor de Internet de la compañía, enviando solicitudes de información a más de 70 MB por segundo, mientras que bajo condiciones normales el servidor de Internet

recibiría solicitudes que llegaban a 2 MB por segundo. Como resultado, el sitio de Internet de la compañía se vio incomunicado de Internet. En ese caso, los delincuentes demandaron y obtuvieron la suma de US $ 40 000, amenazando que, si no se cumplía con sus demandas, continuarían su ataque hasta arruinar completamente a la compañía.

3. También es conveniente fijarnos en el mapa de ataques, amenazas e infecciones cibernéticos registrado por la empresa rusa Kasperky Lab (2 017), en cuyas estadísticas tomadas el 27 de julio de 2 017, figuran Rusia, Alemania, Vietnam, Estados Unidos de América y la India como los países más infectados, ranking que es producto de los análisis efectuados por el antivirus del mismo nombre de la empresa, esto nos revela la escala de intentos de infección de virus en los ordenadores del globo; algunos de estos virus son tipo Hack Tool (manipulación de usuarios del sistema operativo), Dangerous Object (software malicioso), troyanos (acciones maliciosas no autorizadas dentro del software del ordenador), Net-Worm (virus que se propaga por la red sin acción del usuario), entre otros virus que buscan recopilar información o alterar el funcionamiento de los ordenadores para obtener beneficios económicos o para espiar al usuario, sea cual sea el motivo, el número de infecciones y el modo de proceder requieren de mucho conocimiento y de recursos humanos, nos referimos a hackers (cracker) entrenados, equipos de informática (servidores, herramientas de red) , y personal ubicado en distintos países, se trata de una organización criminal, empero, en la sociedad de control, el esfuerzo criminal no se compara con todo el potencial tecnológico que ostentan los Gobiernos de los países más desarrollados de cada Continente, quienes vigilan a sus ciudadanos, incluso son testigos de todo el desarrollo de los inter*criminis* de los delincuentes informáticos, y no hacen nada para no delatarse

frente a otros países, fuera del centro, los países periféricos como los de Latinoamérica, prefieren comprar los software desarrollados por los países del centro, para mantener el control sobre grupos de oposición.

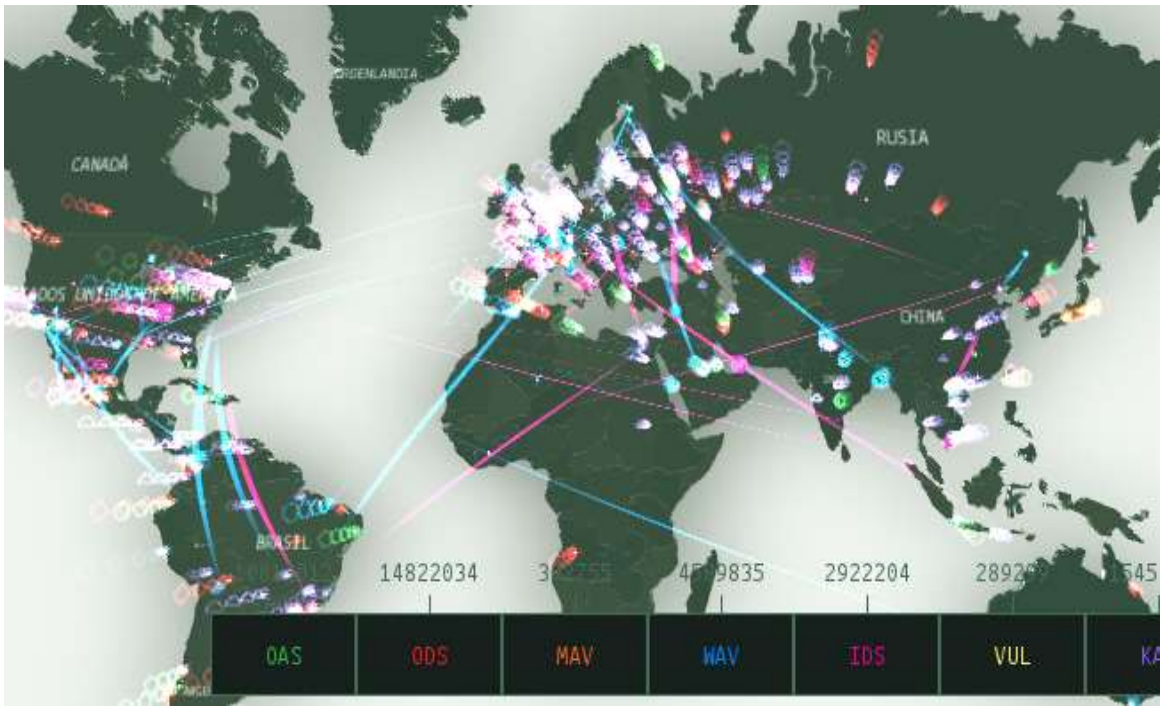

Figura 4. Ciberamenaza: Mapa en tiempo real del 27 de julio de 2 017, donde se aprecia las infecciones detectadas, detenidas o los intentos de infección de virus informáticos, analizadas por el antivirus Kaspersky. Fuente: https://cybermap.kaspersky.com/es

4. Entre todas las características, destacan lo sofisticado, y los perjuicios económicos que pueden ocasionar los delitos informáticos, por lo que nos parece conveniente proponer dos requisitos limitadores, el primero, que el sujeto activo tenga los conocimientos para dominar las TIC que son parte del *iter criminis*, y segundo, que el perjuicio económico sea significativo, de modo que el ámbito de prohibición, sea lo más racionalizado y no devenga en inconstitucional, caso contrario, aumentaría la vulnerabilidad de la población que usa Internet y el resto de tecnologías de manera cotidiana.

§ 4. CLASIFICACIÓN

1. En la Doctrina no hay uniformidad acerca de la clasificación, los criterios tomados para su agrupación son legalistas, técnicos o simplemente arbitrarios, lo que nos da entender que no hay seguridad en los expertos en lo que se quiere estudiar y el cómo estudiarlo, esta ausencia denota la importancia de dotar de un estudio dogmático deslegitimador a los delitos informáticos.

2. En 1 989, Donn B. Parker (p.3-4), expuso una serie de clasificaciones, la *primera*, parte del artículo 1 030 del Código Penal estadounidense, en la que identificó cuatro categorías principales de Delitos Informáticos: 1) La introducción de registros o datos fraudulentos en un sistema informático, 2) Uso no autorizado de instalaciones informáticas, 3) Alteración o destrucción de información o archivos, 4) El robo, por medios electrónicos o de otro tipo, de dinero, instrumentos financieros, propiedad, servicios o datos valiosos; la *segunda*, son categorías generales que se refieren a la manipulación de la información: 1) Por las formas en que ocurre la pérdida de información: Pérdida de integridad, confidencialidad y disponibilidad, 2) Por tipo de pérdida: Daño físico y destrucción por vandalismo, pérdida de propiedad intelectual, pérdida financiera directa y uso no autorizado de servicios, 3) Por el papel desempeñado por las computadoras: Objeto de ataque, entorno único y formas de bienes producidos, instrumento y símbolo, 4) Por tipo de acto relativo a los datos, programas de computadora y servicios: Abuso externo, enmascaramiento, abuso preparatorio, bypass de los controles previstos, abuso pasivo, abuso activo y uso como una herramienta para cometer un abuso, 5) Por tipo de delito: Fraude, robo, hurto, incendio intencional, malversación de fondos, extorsión, conspiración, sabotaje, espionaje y más, 6) Por el *modus operandi*: Ataques físicos, entrada de datos falsos, superzapping, suplantación de

identidad, tapping de hilo, piggybacking, scavenging, ataques de caballos de Troya, uso de trampas, ataques asíncronos, técnicas de salame, fuga de datos, bombas lógicas y simulación, 7) Por habilidades requeridas: No requiere habilidades de programación (barrido físico, espionaje, masquerading, introducción de datos falsos, robo), habilidades de programación requeridas (barrido del sistema, eavesdropping, scanning, piggybacking y tailgating, superzapping, ataques de caballo de Troya, ataques de virus, ataques Salami, usando trapdoors, usando bombas lógicas, ataques asincrónicos, fuga de datos, piratería, uso de empresas criminales).

3. En América Latina, Julio Téllez (2 008, p. 190-191), sostiene que los Delitos Informáticos, se clasifican en dos categorías: (1) *Como instrumento o medio*, que comprenden aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, como a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera), b) Variación de los activos y pasivos en la situación contable de las empresas, c) Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera), d) "Robo" de tiempo de computadora, e) Lectura, sustracción o copiado de información confidencial, f) Modificación de datos tanto en la entrada como en la salida. g) Aprovechamiento indebido o violación de un Código para penetrar a un sistema con instrucciones inapropiadas (método del caballo de Troya), h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa (técnica de salami), i) Uso no autorizado de programas de cómputo, j) Inclusión de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios, k) Alteración en el funcionamiento de los sistemas, l) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos, m) Acceso a áreas

informatizadas en forma no autorizada, n) Intervención en las líneas de comunicación de datos o teleproceso; (2) *Como fin u objetivo,* que se refiere a las conductas dirigidas en contra de la computadora, accesorios o programas como entidad física, como: a) Programación de instrucciones que producen un bloqueo total al sistema, b) Destrucción de programas por cualquier método, c) Daño a la memoria, d) Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados, f) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etcétera).

4. Por su parte Diego Migliorisi (2 014, p.271-272), plantea dos grupos de clasificación: (1) *Delitos típicamente informáticos,* que son aquellos que nunca podrían existir sin la informática y/o Internet, como el hacking, el phishing,el spamming, los hoax, infecciones informáticas por medio de virus o troyanos (programas espías), programas maliciosos destinados a la denegación de servicio, y delitos relacionados con marcas y patentes y la identidad de las personas, como son los casos de mettatanging , typosquatting y cyberquatting (apropiación de dominios de Internet), y (2) *Delitos configurados a través de Internet,* como las calumnias, extorsiones, estafas, hurto informático, violación de correspondencia, instigación a cometer delitos, ejercicio ilegal de la medicina, delitos contra la propiedad intelectual, grooming, cyberbullyng (tipos de acoso), spoofing, incitación a la violencia, y diferentes variantes de delitos sexuales como la pedofilia, pornografía infantil y corrupción de menores.

5. Santiago Acurio (2 007, p. 23-29), prefiere enumerar las acciones o modalidades de delincuencia informática, siguiendo el Manual de Control y Prevención

de Delitos Informáticos de las Naciones Unidas (aunque no lo cita), agrupándolas de la siguiente manera, en (a) Fraudes, (b) Sabotaje informático, (c) Espionaje informático y el robo o hurto de software, (d) Robo de servicios, (e) Acceso no autorizado a servicios informáticos.

6. Los tipos que pertenecen al primer grupo (a) Fraudes, son: *1) Entrada de datos falsos o engañosos (Data Diddling)*, es el método más sencillo, que consiste en cambiar los datos antes o durante su entrada en la computadora, Parker (1 989, p. 12), lo detalla y ejemplifica de la siguiente manera: Cualquier persona asociada o que tenga acceso a los procesos de creación, grabación, transporte, codificación, examen, comprobación, conversión y transformación de datos que en última instancia ingresan a una computadora puede cambiar estos datos. Los usuarios de computadoras autorizadas y confiables que participan en actividades no autorizadas son a menudo las personas que utilizan el método. Un ejemplo típico, es el caso de un empleado de cronometraje que llenó formas de datos de horas trabajadas por 300 empleados en un departamento de la Compañía Ferroviaria. Aprovechó la dicotomía de controles (automatizado por número y manual por nombre del trabajador), llenando los formularios para las horas extraordinarias trabajadas, usando los nombres de los empleados que frecuentemente trabajaban horas extras, pero ingresando su propio número de empleado. Su entrada de datos falsos no fue descubierta por años hasta que por casualidad un auditor que examinó las formas de ingreso federal W-2 notó el ingreso anual inusualmente alto del empleado. Un examen de los archivos informáticos de la hora y los formularios de datos y una discusión con el supervisor del Secretario revelaron la fuente del aumento de los ingresos; *2) Caballos de Troya o manipulación de software*, que consiste en la colocación encubierta o la alteración de las instrucciones de la computadora o los datos

en un programa para que el equipo realice funciones no autorizadas, pero por lo general aún permiten que el programa para realizar la mayoría o todos los fines previstos. (Parker, B.D., 1 989, p. 15); *3) Técnica del Salami,* es una forma automatizada de abuso usando el método del caballo de Troya o ejecutando un programa no autorizado con el fin de tomar pequeñas rebanadas de activos sin reducir notablemente todo. V.gr. en un sistema bancario, el sistema de contabilidad de depósitos a la vista de los programas de cuentas corrientes podría cambiarse (usando el método caballo de Troya) para reducir al azar cada uno de unos pocos cientos de cuentas por 10 centavos o 15 centavos transfiriendo el dinero a una cuenta favorecida donde puede ser retirado a través de métodos autorizados y normales. (Parker, B. D., 1 989, p. 18); *4) Falsificaciones informáticas,* según las Naciones Unidas, se tiene como objeto, cuando se alteran datos de los documentos almacenados en forma computarizada; y, como instrumento, cuando las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. (Magro Servet, V., 2 010, p. 118); *5) Manipulación de datos de la salida,* se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito. (Hall, A. n.d.); *6) La pesca de datos o Pishing y el hurto o robo de identidad (Identity Theft),* el primero consiste en tratar de obtener por fraude, información confidencial como las contraseñas de acceso, haciéndose pasar por una persona o empresa de confianza (Banco) a través de una comunicación electrónica de apariencia oficial (email, sms, página web clonada),

(ITU, 2 009, p. 25), y el *hurto de identidad*, ocurre cuando una persona obtiene datos pertenecientes a otra (la víctima) y se hace pasar por esta última; tiene por objeto, los datos o documentos pertenecientes a otro, para ello es necesario obtener la información, y la necesidad de hacerse pasar por la víctima. (Gercke, M., 2 013).

7.El segundo grupo (b) *Sabotaje Informático*, está integrado por: *1) Bombas lógicas (Logic Bombs)*, se trata de un conjunto de instrucciones en un programa de computadora ejecutado en tiempos apropiados o periódicos en un sistema informático que determina las condiciones o estados de la computadora que facilitan la perpetración de un acto no autorizado y malicioso. (Parker, D.B., 1 989, p. 21-22); 2) *Gusanos* (Worms), son programas que constantemente viajan a través de un sistema informático interconectado sin dañar necesariamente el hardware o el software de los sistemas que visitan. La función principal es viajar en secreto a través de equipos anfitriones recopilando cierto tipo de información programada para enviarla a un equipo determinado al cual el creador del virus tiene acceso. (Roca de Estrada, P., 2 001); 3) Virus informáticos y malware, el *virus informático*, es un conjunto de instrucciones de la computadora que propaga copias o versiones de sí mismo en programas informáticos o datos cuando se ejecuta dentro de programas no autorizados. El virus puede ser introducido a través de un programa diseñado para ese propósito (llamado una plaga) o un caballo de Troya: Las instrucciones ocultas se insertan en un programa informático, los datos o el propio hardware de computadora que utiliza la víctima (Parker, D.B., 1 989, p. 16); en cambio el malware (software malicioso), está diseñado específicamente para obtener acceso o dañar una computadora sin el conocimiento del propietario. (Norton, 2 017). Hay varios tipos de malware (Rivero, M., 2 016), como: i) Adware, que es un software que despliega publicidad de distintos productos o servicios,

agregan íconos gráficos en las barras de herramientas de los navegadores de Internet o en los clientes de correo, ii) Backdoors, que abren una puerta trasera en el sistema para permitir al creador de esta aplicación tener acceso al sistema y hacer lo que desee con él, iii) Botnet, está diseñado para armar una red de equipos infectados por códigos maliciosos, que son controlados por un atacante (ordenador zombi o robor), disponiendo de sus recursos para que trabajen de forma conjunta y distribuida. iv) Hoax, es un correo electrónico distribuido en formato de cadena, cuyo objetivo es hacer creer a los lectores, que algo falso es real, no persigue fines lucrativos como fin principal, v) Hijackers, se encargan de secuestrar las funciones del navegador web (browser) modificando la página de inicio y búsqueda por alguna de su red de afiliados maliciosos, entre otros ajustes que bloquea para impedir sean vueltos a restaurar por parte del usuario, suelen ser parte de los Adwares y Troyanos, vi) Keylogger, se encargan de almacenar en un archivo todo lo que el usuario ingrese por el teclado, se usan para robar contraseñas e información de los equipos en los que están instalados, vii) PUP (Programa potencialmente no deseado), se instala sin el consentimiento del usuario y realiza acciones o tiene características que pueden menoscabar el control del usuario sobre su privacidad, confidencialidad, uso de recursos del ordenador, etc. viii) Rogue, es un programa falso que dice ser o hacer algo que no es, como falsos Antispyware, Optimizadores de Windows, o Antivirus, muestran falsos reportes de infección o problemas, y te piden una versión de pago para resolverlos, ix) Riskware, se trata de programas que ofrecen herramientas de administración remota, que contienen agujeros usados por los crackers para realizar acciones dañinas., x) Rootkit, es malware que puede unirse profundamente en el sistema operativo, en sustitución de los archivos críticos tanto que la eliminación del rootkit podría causar problemas para el sistema operativo, hasta el punto de no poder arrancar; xi) Spam, se trata del correo electrónico

no solicitado enviado masivamente por parte de un tercero; xii) Troyano, es un programa alojado dentro de otra aplicación (un archivo) normal, para pasar inadvertido al usuario e instalarse en el sistema cuando éste ejecuta el archivo "huésped, con el fin de realizar diversas tareas ocultas al usuario, xiii) Spyware (software espía), es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento (ips, navegadores, datos personales, software, etc.), y las remite a servidores (base de datos), con el objetivo de distribuirlo a empresas publicitarias u otras organizaciones interesadas. ix) Ransomware o Secuestradores, se trata de un programa que cifra la información del ordenador y establece unas instrucciones para que el usuario (víctima) pueda recuperar sus archivos, el atacante suele exigir un pago de suma de dinero, para liberar los archivos; 4) Ciberterrorismo, es un terrorismo que no ataca con cargas de explosivos, ni con maletines de gas Sarín (GB), ni con dinamita atada a los cuerpos de fanáticos. Este enemigo nos ataca con uno y cero, en un lugar donde somos más vulnerables: El punto en el que convergen los mundos físico y virtual. (Collin, B.C., n.d). Las Naciones Unidades, sostiene que se usa el Internet para promover y apoyar actos de terrorismo, en particular en forma de propaganda, con fines de reclutamiento radicalización e incitación al terrorismo, además adiestramiento, financiación planificación y ejecución de dichos actos. (2 013, p. 147), sin duda, se cree que el ciberterrorismo es la voluntad de un grupo terrorista de causar muerte o lesiones graves utilizando herramientas de ataque basadas en Internet, o que saboteen sistemas de suministro de luz y agua, de comunicaciones civiles y militares, de gestión bancaria, de transporte (aviones y trenes), de salud, de armamento (Gomez Vieites, 2 014, p. 1-2), y que ésta se encuentra asociada a la *guerra cibernética*, que consisten en las acciones de un Estado para atacar a otro Estado (Lyons, 2 017, April 3), en modesta opinión, se han tomado dichos términos como un cliché de la cultura del

terrorismo para la intervención o fortalecimiento de la sociedad de control tributario del poder de vigilancia del poder punitivo; 5) Ataques de denegación de servicio (DoS, Denial of service), consiste en dejar inaccesible a un determinado recurso, como una servidor web, enviando una gran cantidad de paquetes de forma automática para desbordar los recursos del servidor logrando de esta manera que el propio servicio quede inoperable, si en el ataque están involucrando un gran número de personas que envían paquetes, se trata de un ataque de denegación de servicio distribuido (Distributed Denial of Service o DdoS). (Catoira, F., 2 012). A guisa de ejemplo, la CIA, es la organización que más provecho ha obtenido con el uso del malware, como, el ExpressLane 3.1.1 que, de manera encubierta, se instala como una actualización de seguridad del sistema biométrico oficial de la OTS (Office of Technical Services), con el fin de recolectar información barométrica de la NSA y FBI. (WikiLeaks, 2 017; RT, 2 017, August 24).

8. El tercer grupo (c) Espionaje informático y el robo o hurto de software, está compuesto por: 1) Fuga de datos (Data Leakage), se trata de la fuga o filtración de información confidencial que es accedida por persona ajena a la entidad o empresa, mediante puertos físicos (USB, Wi-Fi, PCMCIA, Bluetooth, HDMI, VGA), o puertos lógicos (correo electrónico, impresiones, capturas de pantalla, Ingeniería Social, códigos maliciosos desarrollados para robar información o explotación de vulnerabilidades de los sistemas) (Mendoza, M. A., 2 016); Secutatis, n.d.; 2) Piratería de programas informáticos, que consiste en realizar copias de programas informáticos sin el consentimiento del titular del Derecho, aquí la lesividad está orientada a los Derechos de Autor.

9. El cuatro grupo (d) Robo de servicios, está integrado por: 1) Hurto del tiempo del ordenador, consiste en el uso sin autorización de un ordenador por un empleado o un tercero, que importa un perjuicio económico para la entidad o empresa proveedora del servicio restringido.(Acurio Del Pino, 2 007, p. 28; Del Peso Navarro, p. 165); 2) Apropiación de información residual (Scavenging), consiste en obtener o reutilizar información de un sistema informático después del procesamiento, mediante métodos técnicos y sofisticados de búsqueda de datos residuales que quedan en una computadora. (Parker, D.B., 1 989, p. 14); 3) Parasitismo informático (Piggybacking), es el acceso no autorizado de una LAN inalámbrica (Wi-Fi), con el propósito de ralentizar la transferencia de datos para los usuarios legítimos de la red, robar datos, diseminación de virus o alguna otra actividad ilícita. (Rouse, M., n.d.); 4) Robo de identidad Suplantación de personalidad (Online Impersonation), consiste en hacerse pasar por otra persona a través de Internet, creando una página web o enviando un correo electrónico o un mensaje instantáneo usando el nombre o nombre de dominio de otra persona con la intención de dañar, defraudar, intimidar o amenazar a otra persona. (All Clear ID, 2 012).

10. El quinto grupo (e) Acceso no autorizado a servicios informáticos, está conformado por: 1) Las puertas falsas (Trap Doors, backdoors), consiste en usar o insertar puertas traseras de programas informáticos, para obtener acceso rápidamente a los sistemas con fines ilícitos, las puertas falsas pueden tratarse accesos creados por el mismo programador para facilitar su tarea, o fallas de programación por olvido o descuido durante su desarrollo. (Northcutt, S., n.d.; UK Essays, 2 015); 2) La llave maestra (Superzapping), es el uso de una aplicación o sistema operativo para montar, leer e incluso escribir valores en elementos de otro sistema operativo, con este programa

es posible leer, crear o borrar archivos y carpetas, es como un programa editor de particiones o sistemas de archivos de un disco duro. (Stanger,J., Lane, P. T.,Crothers, T., 2 002, p. 172); 3) Pinchado de líneas (Wiretapping), consiste en las existen secciones principales del Código Penal Federal que prohíben las intercepciones, revelaciones y capturas de comunicaciones electrónicas, ya sean de línea fija o de telefonía inalámbrica, de voz. La uña o las transmisiones de datos. (Westby, J., 2 003, p. 28); 4) El acceso ilícito a un sistema informático (hacking o craking), se refiere a la intrusión ilegal en un sistema informático o una red, con el propósito de obtener, manipular y destruir información confidencial para ganar dinero (piratería informática) o compartirlo como un Robin Hood. (Cyber Crime Investigation Cell, n.d.; Laws.com, n.d.), en nuestra opinión, este tipo es muy genérico, dado que comprende al resto de actividades delictivas, que requieren el acceso al sistema, por ello es menester racionalizar su aplicación con una interpretación estricta orientado por los Principios de especialidad y de legalidad.

11. Hemos de observar, que la Doctrina, no es uniforme al momento de clasificar los Delitos Informáticos, esto significa que los estudios acerca del panorama delictivo contra las TIC, no son claras, y memos podemos esperar del legislador, quien se vería desorientado por la diversidad de clasificaciones, menuda cuestión, que podría aumentar la vulnerabilidad de la población, en razón que la criminalización primaria no tendría en claro qué es lo que quiere solucionar exactamente, el ámbito de prohibición sería tan amplio que todos seríamos hacker, craker o cualquier enemigo, espía, terrorista, o vulgar delincuente para las agencias ejecutivas ordinarias o especializadas.

§ 5. LOS SUJETOS

1. El *sujeto activo* de los Delitos Informáticos, es cualquier persona, con dominio de lenguajes de programación, hardware de ordenadores, redes de informática, sistemas operativos, Ingeniería Social, etc. (Gomez Vieites, A., 2 014, p. 3), cuya actividad ilícita se denomina hacking propiamente dicho o hacking directo y hacking indirecto (Acosta Patroni, A., 2 003, p. 126-127), el primero se refiere al acceso indebido al sistema; mientras que el segundo, consiste en un acceso como medio para cometer otro tipo de delitos de mayor gravedad, como fraudes, sabotaje, espionaje, etc. En la Doctrina se ha venido caracterizando al agente del delito bajo el título *hacker*, término que en el imaginario popular, denota a jóvenes delincuentes entre 12 y 30 años, solitarios, con poca habilidad social, víctimas de abuso físico o sexual, rebeldes, anarquistas, renegados de la sociedad que actúan con el deseo de satisfacer su ego, compitiendo entre ellos por ser el más grande en romper o evitar sistemas de seguridad informáticos, para otros como simples niños o muchachos inteligentes, cuya curiosidad les encamina a un juego que se convierte en una actividad perniciosa (Rogers, M., n.d., p. 11; Glave, J., 1 999; Molist, M. 2 014, January 11), incluso se llegó a distinguir del cracker (blackhats), que a diferencia de los hackers que solo ponen a prueba su conocimiento sin dañar, éstos serían los verdaderos delincuentes, que atacan los sistemas por razones económicas, políticas y religiosas, también se diferencia; con los años, el delincuente informático, se ha reducido a cualquier sujeto que desde la clandestinidad se dedica a robar información, vaciar cuentas bancarias, sabotear sistemas entre otras actividades; esta cuestión nominal no es óbice para que opere la selectividad del poder punitivo, en tanto que las agencias ejecutivas, prefieran buscar a la presa más fácil, aquel con el estereotipo de hacker, porque el cuello blanco con el poder punitivo es desdibujado, en consecuencia, en un mundo controlado, el más

vulnerable es el desprotegido, el tachado como delincuente por su edad, por su condición económica, por su afición a la tecnología, se trata de un perfil inverso, de alguien sin cuello blanco no es precisamente el verdadero delincuente *white-collar*, que pertenece a una clase socioeconómica alta y a grandes corporaciones, como concluyó Edwin H. Sutherland (2 009, p. 379). Adquiere sentido, el discurso del *white-collar*, cuando el sujeto activo, es el Gobierno, que se vale de sus agencias de inteligencia o seguridad nacional, para vigilar mediante la tecnología y leyes inconstitucionales que habilitan el poder de vigilancia del poder punitivo, con el fin de controlar a los sospechosos y enemigos declarados del Gobierno, sobre todo a dirigentes, periodistas, activistas de derechos humanos, políticos, terroristas y empresarios, para ello, se valen de software y hardware de espionaje, llegando a tener acceso a Cuentas Bancarias, de correo electrónico, de redes sociales y sistemas de gestión judicial, administrativa, tributaria y a toda base de datos que se halle intervenida, con o sin el consentimiento del titular de la información y de la entidad que la conserva en sus servidores de base de datos, en otros casos, contratan hackers, como el caso del iPhone de San Bernardino, que fue crakeado (acceso por la fuerza, rompiendo el acceso con contraseña) por hackers profesionales pagados por el FBI, ante la dificultad de burlar la seguridad de fabricación de Apple, que borraría automáticamente los datos al intentar burlar el sistema de identificación del teléfono móvil, (Nakashima, E. 2 016, April 12), o peor, cuando se trata de grupos de amenazas persistentes avanzadas (APT) orquestadas por los Gobiernos que practican el espionaje de información económica, industrial, de defensa, geopolítica, y de adversarios políticos, como el APT28 de Rusia, la TAO (Tailored Access Operations) de la NSA de Estados Unidos, APT1 (Shangai Group) de China. (Villalón Huerta, A., 2 016, p. 67-70).

2. El *sujeto pasivo*, también es cualquier persona, natural y jurídica (asociaciones, empresas y entidades públicas), titulares de los bienes jurídicos, sobre los cuales recae la actividad típica del agente activo, que presenta la siguiente taxonomía (Ashiq, J. A., 2 005; Gomez Vieites, A., 2 014, p. 3-4; Rogers, M., n.d., p. 8-9; Bosworth, S, Kabay, M. E., Whyne, E. 2 014, p. 405-406): a) Internals (IN, inisider, empelado vengativo), son trabajadores descontentos con acceso privilegiado a un sistema de una organización, es decir que se vale de su posición, puesto, cargo, o relación de confianza respecto del sujeto pasivo, como Gerente, socio, empleado actual o ex empleado, que accede al sistema para facilitar u ocasionar un daño a la información; b) Outsider, es un individuo o un grupo fuera de la organización, que busca obtener información infiltrándose y tomando el perfil de un usuario; c) Sniffers, se dedican a rastrear y recomponer o descifrar los mensajes que circulan por una red local o Internet; d) Phreakers, sabotean las redes telefónicas para realizar llamadas gratuitas; e) Spammers; envían mensajes masivos como correos electrónicos no solicitados, mensajes de texto, o por otro medio, con el fin de publicitar negocios, partidos políticos, ideología, religión y estafar; f) Piratas informáticos, copian programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual; g) Creadores de virus y programas dañinos (Virus Writers [VW]), son programadores de virus que facilitan la comisión de varios delitos informáticos, como la obtención de números de Cuentas Bancarias, tarjetas de crédito, control oculto del hardware y software; h) Lamers (wannabes, script-kiddies, click-kiddies), son aquellas personas que consiguen programas o herramientas para realizar ataques informáticos, lo compran o simplemente lo descargan de Internet; i) Principiante (Novice [NV], Newbie/toolkit), se trata de un delincuente con menor cantidad de conocimientos y destrezas técnicas, que usan scripts (Códigos ejecutables) y herramientas (software de

ataque) para cometer sus crímenes computarizados, j) Cyber Punk (CP), son delincuentes, más avanzados que los principiantes, éstos tienen capacidad de crear scripts y programas de ataque básicos; k) Petty Thieves (PT), son criminales tradicionales y profesionales que usan tecnología actual; l) Old Guard (OG), son criminales informáticos con conocimientos técnicos avanzados y habilidad, sus comportamientos ilegales están motivados por una búsqueda de conocimiento, curiosidad y estimulación intelectual; m) Professional Criminals (PC), son delincuentes que tienen bastante experiencia con la tecnología, pueden se antiguos agentes gubernamentales y de inteligencia motivados por ganancia financiera, son expertos en espionaje industrial; n) Ciberterroristas (Information Warriors), son sujetos altamente calificados que conducen ataques contra los sistemas de información en un intento de paralizar o desestabilizar infraestructura de un Estado.

3. En la llamada sociedad mundial del riesgo, la digitalización significa que: Quien no domina la informática se ve excluido del circuito de la comunicación social (Beck, U., 2 000, p. 83), por ello en la sociedad de control, se difumina la idea de que el hacker o cracker, sea un sujeto con habilidades especiales para la informática. (Acosta Patroni, A. 2 003, p.119), por lo que la taxonomía del hacker, queda soslayada, de modo que el poder punitivo produce una mutación del lego (lammer) a un delincuente informático (hacker), en tanto se sostenga que todos dominamos la informática, así como en estos tiempos nadie duda que uno tenga dominio de la Comunicación y la Matemática, aunque sea la más básica, por ser parte de nuestra vida, nos comunicamos con un idioma, y a diario realizamos operaciones aritméticas; así en la vida digital, toda persona tiene por lo menos un domino básico de las Tecnologías de la Información y la Comunicación (TIC), que lo convierten en un potencial hacker, y por ende la población

legitima el poder de vigilancia, pues en la sociedad de control todos somos sospechosos, a considerarse que esto puede ocasionar un mayor incremento de vulnerabilidad de los habitantes de los países latinoamericanos, pues no se tiene acceso a toda la tecnología de primera, lo que nos mantiene en el *analfabetismo digital*, en razón que el avance del centro es la medida del desarrollo de los países periféricos, que son los segundos o terceros en tener en manos la tecnología y en ser capacitados en su manejo, un ejemplo es la tecnología 4g+ (LTE Advanced) para teléfonos móviles, que apareció en el 2 009 (Parkvall, S., Dahlman, E., Furuskär, A., et al, 2 009), y llegó al Perú el año 2 016 (Gestión, 2 016, July 25), respecto de la última versión de software, llega más rápido en Idioma Inglés, y demorará años en ser actualizado en los ordenadores, por las licencias en el caso de instituciones y empresas, y en los hogares porque no cuentan con los suficientes recursos para comprar un programa informático, situación que mantiene el comercio de productos piratas o las páginas de Warez (sitios web de descargas gratuitas de programas crakeados porque requieren de licencias), a esto el *software libre*, viene a ser una especie de paliativo legal poco usado, salvo por el Sistema Operativo Android en los teléfonos inteligentes (Smartphone) u otras distribuciones de GNU/Linux preinstaladas en computadoras portátiles, además toma años en ser actualizado en el programa de contenidos de Instituciones Educativas dedicadas a capacitar en el uso de estos programas informáticos, por consiguiente, la periferia no ofrece las mejores condiciones para la digitalización y menos para contar con hackers o piratas como del Silicon Valley.

4. Con la finalidad de reducir el poder punitivo, el sujeto activo, debe tener el suficiente dominio del hacking, es decir habilidades para romper sistemas de seguridad y acceder a sistemas informáticos, mediante programación, uso de software para hackear, y manejo de sistemas de redes, quizá, nos traiga problemas aquellos que solo

emplean Ingeniería Social, pues ellos no requieren de conocimientos sofisticados, ellos logran manipular a un tercero para que sea éste quien acceda al sistema y le conceda la ventaja, una solución es el *animus* hacker como componente subjetivo y conocimiento idóneo de cuestiones informáticas para concretar el plan criminal. Un futuro problema, estibará sobre la inteligencia artificial, aquí nace la interrogante si un robot puede ser sujeto activo de un delito, por el momento, opinamos que no, en tanto no se le reconozca como persona, de pronto, solo puede ser considerado una herramienta que toma decisiones, cuyo resultado podrían ser atribuidas a su propietario, por un delito culposo, de todos modos, será de mucha ayuda la interdisciplinariedad con el derecho informático, dado que éste se informa directamente de los avances del conocimiento jurídico con relación a las tecnologías emergentes.

5. Las principales motivaciones de los hackers (Gómez Vieites, A., 2 014, p. 4-5; Burkett, R., 2 013, p. 9-11), son: a) Económicas, pues el dinero es la principal razón por la que se llevan operaciones fraudulentas; robo de información confidencial, extorsiones; intentos de manipulación de las cotizaciones de valores bursátiles, etc.; b) Diversión, porque hay ataques que son realizados sin la finalidad económica; sino como entretenimiento; c) Ideología, por los ataques realizados contra organizaciones por razones políticas, creencias religiosas y nacionalismos; d) Autorrealización, por una sed de reconocimiento social y de un cierto estatus dentro de una comunidad de usuarios de las TIC. Todo lo desarrollado en esta sección, se resumen en la Figura 5.

6. En la Doctrina, existe disquisiciones acerca del bien jurídico, los juristas Santiago Acurio del Pino (2 007, p. 20-22), Luis Miguel Reyna Alfaro (2 002, p. 251-252), Tomás Gálvez Villegas, Walther Delgado Tovar (2 011, p. 1 207-1 208), Felipe Villavicencio Terreros (2 015, p. 6-7), consideran a la información en sus diversas

formas, por su valor económico, personal, por ello concluyen que se trata de una ofensa a varios bienes jurídicos (pluri ofensivo), en ese sentido Gabriel Andrés Campoli (2 013, p. 8), afirma que se protege la intimidad, la información y la propiedad; mientras que Ramiro Salinas Siccha (2 008, p. 1 203) sostiene que el bien jurídico protegido, es la seguridad informática y el patrimonio, en el año 2 017, Laura Mayer Lux, publicó los resultados de una investigación donde expone que son varios los bienes jurídicos propuestos por doctrinarios, como como la calidad, pureza e idoneidad de la información contenida en un sistema informático, el software, Internet, confianza, y otros que se desprende del Convenio de Budapest, ante esto, ella insufla la funcionalidad informática como bien jurídico, en el entendido que se trata de un presupuesto para la realización de diversas actividades de gran relevancia para las personas y las instituciones que están a su servicio en un Estado Democrático de Derecho. (p. 255), al respecto debe considerarse que el Derecho Penal solo recibe los bienes jurídicos ya tutelados por otras ramas del Derecho (Zaffaroni, E. R., 2 016, p. 20), por consiguiente, son la Constitución -la ley penal fundamental- y el Derecho Internacional de los Derechos Humanos, la Fuente de la que emanan todas las relaciones de disponibilidad de una persona con un objeto jurídico tutelado por el Derecho (Zaffaroni, E. R., 2 009a, p. 101), y no cabría elucubraciones provenientes del mismo Derecho Penal, que impidan la realización del Principio de Lesividad, por ello, se debe buscar un bien jurídico, no necesariamente omnímodo para los delitos informáticos; sino reductor del poder punitivo, por tal razón, en nuestra modesta opinión, convendría fijarnos en el Convenio sobre cibercriminalidad a la luz de la Constitución y los Derechos Humanos.

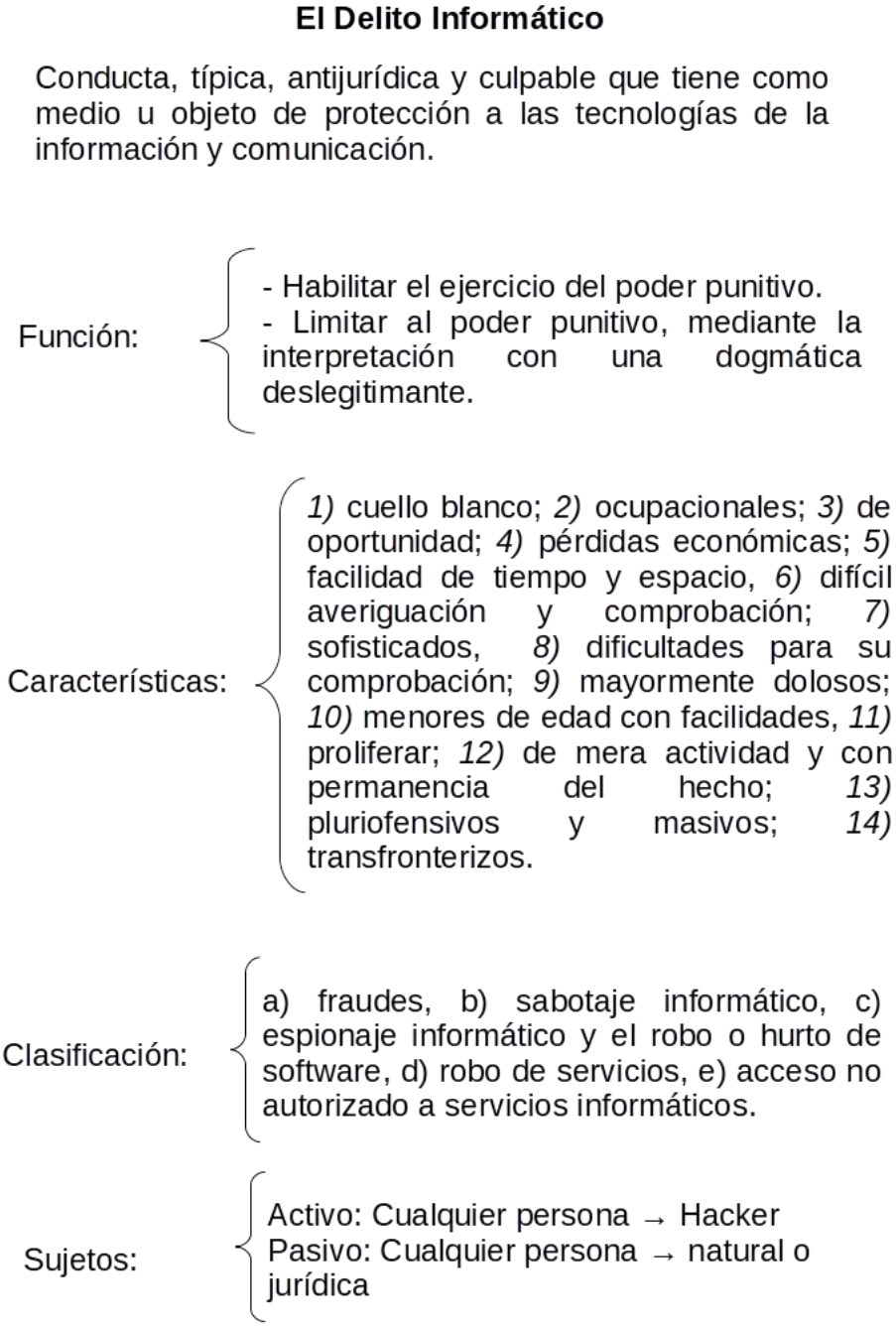

Figura 5. El Delito Informático, definición, función, características, clasificación y sujetos. Fuente: Elaboración propia.

4.5. TRATAMIENTO DE LOS DELITOS INFORMÁTICOS EN EL DERECHO PERUANO Y COMPARADO

§ 1. CONSIDERACIONES GENERALES

1. Los Delitos Informáticos en el ordenamiento jurídico peruano, están previstos en la Ley 30 096 "Ley de Delitos Informáticos", modificado por la Ley 30 171; y en el Derecho Comparado, se encuentran regulados por diversas leyes especiales heterogéneas o en el mismo Código Penal de países como, Estados Unidos, Alemania, Francia, España, Chile, Argentina y Ecuador. Naciones que elegimos para el presente estudio, su legislación y la del Perú, fue la sustancia sobre la cual se procedió con el análisis histórico-comparativo, que despliega un análisis genealógico sobre los Delitos Informáticos contemplados en la legislación peruana y la legislación comparada con los mencionados países, con la finalidad de deslegitimar al poder punitivo en la sociedad de control, con ello proponemos una Doctrina reductora conforme al derecho penal humano expuesto por el maestro Raúl Zaffaroni, para conseguir orientar en la decisiones jurisdiccionales sobre delitos que habilitan el poder punitivo sobre conductas que afectan sistemas, datos informáticos y otros bienes jurídicos asociados a las Tecnologías de la Información y Comunicación (TIC).

2. El orden de exposición, se da según la ley de delitos informáticos del Perú, y cada delito integra en su análisis, citas de legislación comparada para efectos de arribar a una conclusión sobre los intereses del legislador histórico y las distintas formas de tipificación, para ello seguimos el tradicional estudio estratificado que va desde lo histórico, pasando por el sustantivo, a lo adjetivo del delito, esto es la forma de análisis del maestro Zaffaroni para la parte especial del Derecho Penal, quien afirma que los tipos arrastran una genealogía originaria, que pasa a otro contexto temporo - espacial,

que es adoptado por otro legislador histórico (2 009b, p. 18). La presente investigación se plegó a la óptica reductora del poder punitivo.

§ 2. ACCESO ILÍCITO

1. **Genealogía y Derecho Comparado:** La protección de los sistemas informáticos, surge en 1 977, con el Senador norteamericano Abraham Ribicoff [D., Conn], quien tuvo la iniciativa legislativa con la presentación del Proyecto de la "Federal Computer Systems Protection Act", para que los delitos informáticos sean un delito federal, con la finalidad de proteger los datos confidenciales de hospitales, compañías de seguro, secretos comerciales, Bancos, seguridad nacional (Secretos de Estado). El mencionado Proyecto no fue aprobado, y recién el 12 de octubre de 1 984, el Congreso de los Estados Unidos, promulgó la Ley "Counterfeit Access Device and Computer Fraud and Abuse Act", que incorporó la §1 030. "Fraud and related activity in connection with computers", ubicado en el Capítulo 47, parte 1, Título 18 del Código Federal de los Estados Unidos, esta ley prohibió el uso no autorizado o el acceso a las computadoras sin autorización para obtener: a) Información clasificada de los Estados Unidos, con la intención o razón de creer que dicha información será utilizada para dañar a los Estados Unidos o para beneficiar a una Nación extranjera; b) Información financiera o crediticia que esté protegida por las leyes federales de privacidad financiera; c) Para utilizar, modificar, destruir o divulgar cualquier información en el mismo, o impedir que otros utilicen el ordenador; asimismo, la ley también prohíbe cualquier intento o conspiración para cometer cualquiera de estos supuestos.[3]

3 §1030. Fraud and related activity in connection with computers(a) Whoever- (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) 1 of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); (B) information from any department or agency of the United States; or (C) information from any protected computer.

(Tompkins Jr., J. B. & Mar, L. A., 1 986, p. 460-461; Washingtonpost, 2 003; Kelly, H., 1 977, June 28, p. 36); tales prohibiciones, nacieron en medio de la guerra fría, por tanto el legislador, pretendía evitar la fuga de información confidencial del Gobierno y de las empresas hacia manos de los enemigos, puesto que la protección de los Secretos de Estado y empresariales, fueron parte de una estrategia geopolítica para la construcción de la sociedad global de la información, como afirma Matterlart (2 002, p. 12), siendo así, las informaciones libres, las que se dejaron fuera de la prohibición penal, y que son creadas por el marketing, los medios de comunicación, la propaganda, se fomentaron para mantener el *soft power*, que lleva a aceptar normas e instituciones que producen un comportamiento deseado por el Estado, para que su poder sea legítimo a los ojos de los demás; a su vez, el *Cyberwar (Cyberwafare)* y la *Netwar*, que son conflictos de alta y baja intensidad protagonizados por actores estatales y no estatales (guerrilleros, carteles, etc.), generaron el temor de la electronic Pearl Harbor (p. 136-137), en esta coyuntura, se fue forjando el estereotipo del hacker, quien podría acceder o dañar a los sistemas informáticos y divulgar toda la información sobre la tecnología militar y secretos empresariales, como sucedió en la película War Games de John Badham (Filmaffinity, 1 983), la historia del adolescente que ingresa a un sistema de mandos de misiles nucleares y la cultura del terrorismo alimentaron el estereotipo, desde luego, las agencias de seguridad nacional (inteligencia) se convirtieron en los cerebros de los aparatos de gobierno en la sociedad de control, su actividad se intensificó con el atentado del 11 de setiembre de 2 001 en Estados Unidos, con ello los países se han preocupado en conformar un sistema inteligencia global, que es todo un panóptico global.

2. En Alemania, el acceso ilícito, fue sancionado con el *nomen juris* "Ausspähen von Daten" (espionaje de datos) ubicado en la § 202a del Código Penal Alemán[4], añadido el 22 de diciembre de 1 987 (Marquez Valencia, A.D., 2 012), a diferencia de los Estados Unidos, resta toda mención literal a instituciones o empresas, empleando una fórmula genérica, para los sujetos y para describir la conducta: "Cualquier persona que no esté autorizada o tenga acceso a datos que no estén destinados a él y que esté especialmente protegida contra el acceso no autorizado, con la superación de la seguridad de acceso. (...)"; y el 05 de enero de 1 988 en Francia se penalizó el acceso fraudulento (Art. 462-2), mediante la Ley 88/19 (Segu.Info, n.d.), que sanciona el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema; posteriormente en 1 994, se dicta en el nuevo Código Penal Francés, que sustituyó al Código Napoleónico de 1 810 (Marti, O., 1 994, March 2), este nuevo Código consideró al acceso ilícito en el artículo 323-1[5], sancionando el acceder o mantener, de forma fraudulenta, en todo o parte de un sistema automatizado de tratamiento de datos, con la agravante si resulta la supresión o modificación de datos o la modificación del funcionamiento del sistema, asimismo cuando se comete contra un sistema automatizado de tratamiento de datos de carácter personal por el Estado.

4 § 202a Ausspähen von Daten (1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

5 Article 323-1 Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4.
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende. Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

3. En Chile, el 07 de junio de 1 993, se sancionó la Ley 19 223, que en su artículo 2 penaliza al "que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él", de modo que se enfatizó el aspecto subjetivo a diferencia del resto de tipos penales que hemos revisado; resulta diferente en España, donde el Rey Juan Carlos I, el 23 de noviembre de 1 995, sancionó la Ley Orgánica 10/1 995, en el primer párrafo del artículo 197 bis del Código Penal Español, que establece: "El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo (...)", deja al intérprete la tarea de inferir el aspecto subjetivo, sin precisar el ánimo que requiere. En México, el 17 de mayo de 1 999, se publica un Decreto que reforma diversas disposiciones en materia penal, la cual integra en el Título Noveno del Código Penal, el Capítulo ii sobre acceso ilícito a sistemas y equipos de informática, diversificando la fórmula legal genérica alemana en varios artículos que van desde el artículo 211 bis 1 al 211 bis 7, que penaliza al que con o sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad. En el Perú, el 17 de julio de 2 000, se publicó la Ley 27 309 "Ley que incorpora los Delitos Informáticos al Código Penal", que modifica el Título V para integrar los Capítulos X y XI con los artículos 207-A, 207-B y 207-C, aunque el artículo 1 de la Ley 26 319, publicada el 01 de junio de 1 994, modificó el artículo 186 del Código Penal, adicionando una modalidad de Hurto Agravado mediante sistemas electrónicos o telemáticos[6] que en su momento, fue el único Delito Informático en el Perú; en cuanto al acceso ilícito, éste se

6 186.- 3. Mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas.

encontró originariamente en el artículo 207-A, sin *nomen juris*, en ninguno de los proyectos de ley se hizo mención de ella, tampoco en los debates[7], por lo que la Doctrina no es uniforme en su denominación (Reyna Alfaro, L. M, 2 002, p. 257; Salinas Siccha, R., 2 008, p.1 199, Peña Cabrera Freyre, A. R., 2 015, p. 725; Gálvez Villegas, T. A., Delgado Tovar, W. J., 2 011, 1 209) los juristas lo denominaron como "Espionaje Informático", "Instrusionismo Informático", "Ingreso indebido a base de datos y sistemas", la fórmula legal decía, "El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, (...)", con la agravante que "Si el agente actuó con el fin de obtener un beneficio económico (...)", y del artículo 207-C que señala que "En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional.".

4. En Ecuador, se siguió una fórmula legal similar a Estados Unidos y México, para ello, en el 2 002 se reformó el Código Penal Ecuatoriano con la Ley 2 002-67, por el cual incluyen a continuación del artículo 202 diversos artículos sin numeración, uno de ellos decía "El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad (...)". con las agravantes: "Si la

7 Fueron tres los proyectos de ley, con los números 0507/99, 05132/99, 05326/99, presentados en los años 1 999. Los debates se realizaron el 03 mayo y 21 de junio de 1 999.

información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, (...). La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, (...). Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, (...)", actualmente, se denomina "Acceso no consentido a un sistema informático, telemático o de telecomunicaciones" y se ubica en el artículo 234 del Código Orgánico Integral de Ecuador (2 014), cuyo texto señala "La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, (...)".

5. En Argentina, en el año 2 008, el art. 5 de la Ley 26 388, incorporó al Código Penal Argentino, diversos artículos sobre Delitos Informáticos, entre ellos el artículo 153 bis: que sanciona penalmente al que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido, con la agravante, cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros. En nuestro país, el 22 de octubre del 2 013, se publicó en el Diario Oficial el Peruano, la Ley de Delitos Informáticos: Ley 30 096, con Fe de Erratas publicado al día siguiente en una edición extraordinaria del mencionado Diario, el acceso ilícito ubicado en el artículo 2 de la mencionada ley, tuvo el siguiente texto: "El que accede sin autorización a todo o parte de un sistema informático, siempre

que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado".

6. La adopción o la compatibilidad con los criterios del Convenio de Budapest "Convenio sobre la Ciberdelincuencia" (Council of Europe, 2 001), fue uno de los fundamentos de los Proyectos de Ley con los números 03105/2 013-CR, 03048/2 013-CR, 03017/2 013-CR 2 999/2 013-CR, 2 991/2 013-CR, además se dijo que era menester precisar mejor las conductas, mejorar la cooperación entre la Policía y otras entidades para la mejor persecución del delito, y se enfatizó que las conductas deben ser deliberadas e ilegítimas, por ello creemos que tanto el *nomen juris* y la fórmula legal del acceso ilícito provino literalmente del citado Convenio traducido al español a la Ley 30 171 que modificó la Ley 30 096, y se mantuvo la agravante por exceder lo autorizado (que proviene de la fórmula legal de Estados Unidos), para comprobar ello, revisemos el texto del Convenio, que dice:

> "Artículo 2. Acceso ilícito. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático."; y el artículo 2 de la Ley de Delitos Informáticos (Ley 30 096), cuyo texto dice:

"**Artículo 2. Acceso ilícito**

"El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado."

7. **Balance histórico:** a) Sobre la naturaleza del delito, el acceso ilícito, es un tipo que surge como una forma de espionaje contra el Estado, y transita por diversos países hasta convertirse en un delito informático que atañe a sujetos comunes, no siendo siempre el Estado y las empresas el sujeto pasivo; b) El contenido del injusto del hecho típico, nació como un tipo de baja gravedad, y comparativamente con la penalidad en países de Latinoamérica (Riquert, M. A., 2 014, p. 232), observamos que hay una tendencia a incrementar el máximo del marco abstracto de la pena, bajo el argumento que la comisión y los daños son equiparables a los delitos comunes, en el caso del acceso, equivaldría a que un delincuente ingrese a una casa y hurte documentación de los archivadores; c) Requisitos típicos más notorios, el sujeto pasivo inicialmente solo era el Estado y las empresas, luego se extendió a cualquier persona.

8. El tipo nació en una coyuntura bélica, en la que los Gobiernos debían proteger los secretos de Estado y de la empresa, tributarios necesarios para financiar la carrera armamentista, en ese contexto, tenía un sentido de protección contra el espionaje, posteriormente, cuando la comunicación por ordenadores se masificó, el tipo, cobró un

sentido de protección contra el acceso indebido e ilegítimo a los sistemas informáticos públicos y privados de cualquier persona.

9. En el Perú, el acceso ilícito aparece con la Ley 27 309, que incorporó los Delitos Informáticos al Código Penal peruano, eclosiona en medio de un Gobierno dictatorial y corrupto de Fujimori y Montesinos (López Martínez, H., 2 011, p. 68, 72; Palacios Rodriguez, R., 2 014, p. 245-247, 254), el ex presidente Alberto Fujimori Fujimori, bajo esa línea autoritaria, mediante una observación a la Autógrafa de la citada Ley, propuso regular como agravante y con mayor severidad cuando el sujeto pasivo sea una organización de defensa nacional, seguridad interior, inteligencia, o cuando se afecte la seguridad de la Nación, asimismo cuando el agente en razón de su cargo o puesto de trabajo tuviere acceso a información clasificada o privilegiada, y se aprovecha para cometer el delito. (Fujimori Fujimori, A. 2 000, May 30), propuesta que emergió como reflejo de una ideología heredada de la guerra fría, que con el artículo 207-C permeó de algún modo en la legislación peruana, la que estableció hasta el año 2 013, que en los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional, similar agravante se tiene el artículo 11 de la Ley de Delitos Informáticos.

10. **Tipo objetivo. Los sujetos:** El sujeto activo, es cualquier persona natural, no se exige alguna condición especial o relación con el sujeto pasivo y el sistema informático; en cuanto al sujeto pasivo, éste puede ser una persona natural o jurídica. La Doctrina nacional, sostiene que el sujeto activo debe tener conocimientos de informática

necesarios para la acción típica (Reyna Alfaro, L. M, 2 002, p. 258; Salinas Siccha, R., 2 008, p. 1 203, Peña Cabrera Freyre, A. R., 2 015, p. 725-726; Gálvez Villegas, T. A., Delgado Tovar, W. J, 2 011, 1 209).

11. Originariamente, el agente activo solo era un hacker, el delincuente de cuello blanco, y el pasivo, el Estado y la Empresa, con la comercialización de las TIC, el ámbito de prohibición se amplió, ocasionando un cambio cualitativo en los sujetos en el Convenio de Budapest, que influyó en el legislador peruano.

12. Tipo objetivo sistemático. La exteriorización de la acción: Según el artículo 1, literal "a" del Convenio de Budapest, se entenderá por «sistema informático» a todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa; el tipo prohíbe el acceso a todo o en parte a dicho sistema informático de manera deliberada e ilegítimamente, por no decir intencionada y en contra del ordenamiento jurídico, con la agravante de acceder en todo o en parte al sistema informático, excediendo lo autorizado, es decir usar los privilegios de lectura en información que está fuera del ámbito establecido por el IT Manager, o directivas de gestión del sistema informático.

13. La conducta de acceder en todo o en parte, que es de mera actividad (Villavicencio Terreros, F., 2 015), por tanto se consuma con solo ingresar o entrar a una zona de acceso restringido que es parte del sistema informático de manera parcial o total, vulnerando la seguridad establecida, o contando con los privilegios para ingresar, excede entrando a espacios no permitidos, en el primer supuesto, la vulneración puede realizarse con la ejecución de programas informáticos dedicados a romper la seguridad,

o simplemente con técnicas de Ingeniería Social que revele los datos de acceso, ello implica dar uso a privilegios no concedidos, en el segundo supuesto, el acceso se da porque el agente cuenta con los privilegios para ingresar al sistema informático hasta cierta zona o parte del mismo, pero aprovechando ello, decide deliberada e ilegítimamente usar dichos privilegios para ingresar.

14. A guisa de ejemplo, para el primer supuesto, según el Diputado Lee Cheol-hee, "hackers" de Corea del Norte, entraron al Centro Integrado de Documentación de Defensa de Seúl en setiembre del año 2 016 para robar 235 gigas de información militar clasificada, que incluía planes de operaciones conjuntas de los ejércitos de Corea del Sur y EE.UU. (DW, 2 017, October 11), en este caso no se precisa los medios, pero de cualquier forma se produjo el resultado lesivo; y para el segundo supuesto, podemos imaginar que un empleado del Poder Judicial, que tiene una cuenta de acceso a un sistema informático, con privilegios de lectura de diversos módulos sobre manejo de expedientes, empero, su función solo está limitada a brindar información pública a los justiciables sobre el estado del expediente judicial, pero éste accede proyectos de sentencias almacenadas en el sistema informático.

15. La vulneración de las medidas de seguridad, siendo un requisito importante la de verificarse, además del dominio informático del agente activo para romper la seguridad con los debidos exámenes periciales por especialistas en seguridad informática, de no acreditarse la vulneración o el exceso en los permisos concedidos, el hecho será atípico, verbigracia, una persona observa que el CPU de un ordenador está funcionando, se acerca, mueve el ratón, y se enciende la pantalla, y observa el texto de correo electrónico abierto, o mensaje de Facebook u otra plataforma visual, en este caso,

el sujeto accede a la información sin vulnerar las medidas de seguridad, se trata de una negligencia del propietario de la información, que no cerró su correo electrónico o cuenta de mensajería, tampoco sería un asunto de exceso, puesto que el agente nunca tuvo privilegios de acceso al sistema, por tanto no tendría oportunidad de exceder de dichos permisos; ahora bien, las acciones que sucedan al hecho atípico, pueden ser abarcados por otro ámbito de prohibición, como eliminar la información, estaríamos frente al delito de atentado a la integridad de datos informáticos.

16. **Tipo objetivo conglobante. Bien jurídico**: La confidencialidad de datos y sistemas informáticos, es el bien jurídico que debe ser ofendido o afectado, ello se desprende del Título 1. del Capítulo II del Convenio sobre la ciberdelincuencia: "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"; dado que el Derecho Penal es sancionador y no constitutivo de bienes jurídicos (Zaffaroni, E. R., 2 016), creemos que este bien jurídico, se funda en el derecho fundamental a la confidencialidad e integridad de sistemas informáticos, desarrollado por el Tribunal Constitucional Federal Alemán en los casos BvR 370/07 - 1 BvR 595/07, como una especie de derivación del derecho fundamental a la personalidad (Persönlichkeitsrecht) (Manssen, G., 2 014, June, p. 39), ubicado en el artículo 22 de la Declaración Universal de Derechos Humanos, el inciso 1 del artículo 2 de la Constitución peruana, por la importancia de las computadoras. Internet, teléfonos móviles y las tecnologías para el desarrollo de la personalidad, puesto que el desarrollo reciente de la tecnología de la información ha hecho que los sistemas de tecnología de la información se vuelvan omnipresentes, y su uso es vital para las vidas de muchos ciudadanos.

17. **Tipo subjetivo:** El *dolo*, es la voluntad realizadora del tipo guiada por el conocimiento de los elementos del tipo objetivo sistemático (Zaffaroni, E. R., 2 009a, p. 108), por ello el agente, que actúa deliberada e ilegítimamente, debe saber y querer acceder a todo o en parte a un sistema informático, vulnerando las medidas de seguridad, o conocer los límites establecidos por el IT Manger, y exceder de lo autorizado con el *animus hacking*, que se trata de la finalidad de romper la seguridad para acceder al sistema informático, caso contrario, no hay dolo, verbigracia, si un empleado de limpieza sin conocimientos en informática, realiza una limpieza del teclado y ratón un ordenador de escritorio encendido, y al llegar el sujeto pasivo, se da cuenta que accedieron sin autorización a un sistema de manejo de armas nucleares, su conducta será atípica, pues si bien logró acceder, no hubo voluntad realizadora ni conocimiento del tipo objetivo sistemático.

18. El artículo 12 de la Ley 30 096, ha establecido una exención de responsabilidad penal cuando el acceso a todo o en parte al sistema informático, se produce con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos; se trata del Penetration Testing (PenTesting), que es una simulación de ataque a un sistema informático, red, o equipos para demostrar vulnerabilidades en caso de un ataque real (Henry, K. M., 2 012, p.12), la cual debe contar con la debida autorización del administrador de los sistemas informáticos, opinamos que ésta al ser parte de todo un procedimiento técnico, por no decir informal, no es necesario contar con una autorización escrita, basta con una orden verbal, opinamos que la actuación sí debe consignarse en algún acta, informe o similar donde se reporte las vulnerabilidades; en este supuesto, el agente actúa con el *animus hacking*, pero lo realiza autorizado por el mismo sujeto pasivo, para encontrar vulnerabilidades, es como una especie de aquiescencia, que podría ubicarse en los

términos del contrato o directivas de instalación o mantenimiento de los equipos informáticos, de cualquier manera los problemas que se susciten respecto de ellos, son parte de la esfera privada o administrativa.

19. Concurrencia y participación: Eventualmente, puede producirse una concurrencia con los delitos de atentado contra los datos informáticos, o sistemas informáticos, puesto que ambos casos según la técnica de hacking, y por el modo de atentar se necesita acceder al sistema, para dañar los datos estando adentro, igual para inutilizar el sistema, salvo que se trate de impedir el acceso, en ese supuesto se puede impedir el acceso al sistema informático, tanto desde adentro o afuera, de todos modos; si el ataque es desde adentro, en una primera fase se tuvo que acceder o exceder de los permisos concedidos.

20. Este tipo penal, admite la coautoría, y la participación de cómplices e instigadores; creemos que los coautores pueden realizar aportes necesarios para la ejecución de la conducta típica, verbigracia, que uno de ellos se ocupe en averiguar el "user" y el otro el "password" de la cuenta a la que pretenden ingresar, por supuesto que esto demanda determinar el dominio funcional del hecho, y en el caso de la autoría mediata, el dominio de la voluntad del otro.

§ 3. ATENTADO A LA INTEGRIDAD DE DATOS INFORMÁTICOS

1. **Genealogía y Derecho Comparado:** El 12 de octubre de 1 984, el Congreso de los Estados Unidos, promulgó la ley "Counterfeit Access Device and Computer Fraud and Abuse Act", que incorporó la §1 030. "Fraud and related activity in connection with computers", ubicado en el Capítulo 47, parte 1, Título 18 del Código Federal de los Estados Unidos, esta ley prohibió además el uso no autorizado o el

acceso a las computadoras sin autorización, el modificar, destruir o divulgar cualquier información del mismo.[8] (Tompkins Jr., J. B. & Mar, L. A., 1 986, p. 460-461; Washingtonpost, 2 003; Kelly, H., 1 977, June 28, p. 36); tales prohibiciones, nacieron en medio de la guerra fría, por tanto el legislador, tenía la intención de cautelar la integridad de la información accedida de forma indebida.

2. En Alemania, el atentado a la integridad de datos informáticos, fue sancionado con el *nomen juris* "Datenveränderung" (modificación de datos) ubicado en la § 303a del Código Penal Alemán[9], a diferencia de los Estados Unidos, la conducta es más clara y dirigida al daño de los datos; y el 05 de enero de 1 988 en Francia se penalizó la destrucción de datos (Art. 462-4), mediante la Ley 88/19 (Segu.Info, n.d.), que sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión; posteriormente en 1 994, se dicta en el nuevo Código Penal Francés, que sustituyó al Código Napoleónico de 1 810 (Marti, O., 1 994, March 2), este nuevo Código consideró la destrucción de datos en el artículo 323-3[10], sancionando la introducción fraudulenta

8 §1030. Fraud and related activity in connection with computers(…) (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss. (...).

9 § 303a Datenveränderung (1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. (2) Der Versuch ist strafbar.(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

10 Article 323-3 Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4 Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

de datos en un sistema de procesamiento automatizado para extraer, poseer, reproducir, transmitir, eliminar o modificar de manera fraudulenta los datos que contiene el sistema.

3. En Chile, el 07 de junio de 1 993, se sancionó la Ley 19 223, que en su artículo 3 penaliza "al que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información"; en España, el Rey Juan Carlos I, el 23 de noviembre de 1 995, sancionó la Ley Orgánica 10/1 995, en el artículo 264 del Código Penal Español, que establece: "1. El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años". En México, el 17 de mayo de 1 999, se publica un Decreto que reforma diversas disposiciones en materia penal, la cual integra en el Título Noveno del Código Penal, el Capítulo ii sobre acceso ilícito a sistemas y equipos de informática, diversificando la fórmula legal genérica alemana en varios artículos que van desde el artículo 211 bis 1 al 211 bis 7, que penaliza al que con o sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado y de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. En el Perú, el 17 de julio del 2 000, se publicó la Ley 27 309 "Ley que incorpora los Delitos Informáticos al Código Penal", que contempla el daño de datos y la interceptación ilícita en el artículo 207-B, sin *nomen juris*, en ninguno de los Proyectos de ¨Ley se hizo mención de ella, tampoco en los debates[11], por lo que la Doctrina no es uniforme en su denominación (Reyna Alfaro, L. M, 2 002, p. 260; Salinas Siccha, R., 2 008, p.1 206, Peña Cabrera Freyre, A. R.,

11 Fueron tres los Proyectos de Ley, con los números 0507/99, 05132/99, 05326/99, presentados en los años 1 999. Los Debates se realizaron el 03 mayo y 21 de junio de 1 999.

2 015, p. 729; Gálvez Villegas, T. A., Delgado Tovar, W. J., 2 011, 1 217) los juristas lo denominaron como "Sabotaje Informático", "Alteración, daños, destrucción de la información y la base de datos", la fórmula legal decía, "El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.", con la agravante del artículo 207-C "En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional.".

4. En Ecuador, con la Reforma del 2 002 al Código Penal Ecuatoriano, mediante la Ley 2 002-67, se incluyó el artículo 415 el siguiente texto "Daños informáticos. - El que dolosamente, de cualquier modo, o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica. La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional", actualmente, se denomina "Ataque a la integridad de sistemas informáticos" y se ubica en el artículo 232 del Código Orgánico Integral de Ecuador (2 014), cuyo texto señala "La persona que destruya, dañe, borre, deteriore, altere,

suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años".

5. En Argentina, en el 2 008, el art. 5 de la Ley 26 388, incorporó al Código Penal Argentino, diversos artículos sobre delitos informáticos, entre ellos el artículo 183: Que reprime al que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. En nuestro país, el 22 de octubre de 2 013, se publicó en el Diario Oficial el Peruano, la Ley de Delitos Informáticos: Ley 30 096, con Fe de Erratas publicado al día siguiente en una edición extraordinaria del mencionado Diario, el atentado a la integridad de datos informáticos fue ubicado en el artículo 3 de la mencionada ley, tuvo el siguiente texto: "El que, a través de las Tecnologías de la Información o de la Comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

6. La adopción o la compatibilidad con los criterios del Convenio de Budapest "Convenio sobre la Ciberdelincuencia" (Council of Europe, 2 001), fue uno de los fundamentos de los Proyectos de Ley con los números 03105/2 013-CR, 03048/2 013-CR, 03017/2 013-CR 2 999/2 013-CR, 2 991/2 013-CR y habiéndose tomado como texto base, la fórmula legal del atentado a la integridad de datos provino literalmente del

citado convenio traducido al español a la Ley 30 171 que modificó la Ley 30 096, para comprobar ello, revisemos el texto del Convenio, que dice:

> "Artículo 4. Interferencia en los datos"
>
> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
>
> 2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.
>
> El artículo 2 de la Ley de Delitos Informáticos (Ley 30 096), cuyo texto dice:
>
> "**Artículo 3. Atentado a la integridad de datos informáticos**"
>
> El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

7. **Balance histórico:** a) Sobre la naturaleza del delito, el atentado a la integridad de datos informáticos, es un tipo que surge como una conducta derivada del espionaje contra el Estado, y transita por diversos países hasta convertirse en un delito informático que atañe a sujetos comunes, no siendo siempre el Estado y las empresas el sujeto pasivo; b) El contenido del injusto del hecho típico, nació como un tipo de baja gravedad, y comparativamente con la penalidad en países de Latinoamérica (Riquert, M.

A., 2 014, p. 232), observamos que hay una tendencia a incrementar el máximo del marco abstracto de la pena, bajo el argumento que la comisión y los daños son equiparables a los delitos comunes, en el caso del atentado contra los datos, equivaldría a que un delincuente ingrese a una casa y queme o altere la documentación de los archivadores; c) Requisitos típicos más notorios, que el sujeto activo debe atentar contra los datos informáticos que pueden ser ficheros, bases de datos, programas informáticos, es decir solo el soporte lógico, queda fuera de la prohibición típica el hardware que es parte de los sistemas informáticos.

8. El tipo nació en una coyuntura bélica, en la que los Gobiernos debían proteger los secretos de Estado y de la empresa, tributarios necesarios para financiar la carrera armamentista, en ese contexto, tenía un sentido de protección contra el espionaje y sabotaje, posteriormente, cuando la comunicación por ordenadores se masificó, el tipo, cobró un sentido de protección contra datos de los sistemas informáticos públicos y privados de cualquier persona.

9. En el Perú, el atentado contra datos informáticos aparece como una especie de sabotaje informático con la Ley 27 309, que incorporó los delitos informáticos al Código Penal peruano, la misma que eclosiona en medio de un Gobierno dictatorial y corrupto de Fujimori y Montesinos (López Martínez, H., 2 011, p. 68, 72; Palacios Rodriguez, R., 2 014, p. 245-247, 254), el ex presidente Alberto Fujimori Fujimori, bajo esa línea autoritaria, mediante una observación a la Autógrafa de la citada Ley, propuso regular como agravante y con mayor severidad cuando el sujeto pasivo sea una organización de defensa nacional, seguridad interior, inteligencia, o cuando se afecte la seguridad de la Nación, asimismo cuando el agente en razón de su cargo o puesto de

trabajo tuviere acceso información clasificada o privilegiada, y se aprovecha para cometer el delito. (Fujimori Fujimori, A. 2 000, May 30), propuesta que emergió como reflejo de una ideología heredada de la guerra fría, que con el artículo 207-C permeó en la legislación peruana, la que estableció hasta antes del año 2 013, que en los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional; y después del año 2 013, lo sucedió - en esta política criminal - el artículo 11 de la Ley de delitos informáticos, cuando le da mayor reproche penal al agente el delito al comprometer fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

10. **Tipo objetivo. Los sujetos:** El sujeto activo, es cualquier persona natural, no se exige alguna condición especial o relación con el sujeto pasivo y el sistema informático; en cuanto al sujeto pasivo, éste puede ser una persona natural o jurídica. La doctrina nacional, sostiene que el sujeto activo debe tener conocimientos o habilidades de informática necesarios para la acción típica (Reyna Alfaro, L. M, 2 002, p. 261; Salinas Siccha, R., 2 008, p.1 210, Peña Cabrera Freyre, A. R., 2 015, p. 729-730; Gálvez Villegas, T. A., Delgado Tovar, W. J., 2 011, 1 217).

11. Originariamente, el agente activo solo era un hacker, el delincuente de cuello blanco, y el pasivo, el Estado y la Empresa, con la comercialización de las TIC, el ámbito de prohibición se amplió, ocasionando un cambio cualitativo en los sujetos en el Convenio de Budapest, que influyó en el legislador peruano.

12. El artículo 11 de la Ley de Delitos Informáticos, le da mayor reproche penal al agente, cuando es integrante de una organización criminal, abusa de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

13. Tipo objetivo sistemático. La exteriorización de la acción: Según el artículo 1, literal "b" del Convenio de Budapest, se entenderá por «Datos Informáticos», cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función; el tipo prohíbe la afectación a los datos informáticos o hacerlas inaccesibles, que sería una de las acciones asociadas al Sabotaje Informático que han de realizar de manera intencionada y contra las prohibiciones del Ordenamiento Jurídico, ahora bien, examinemos los verbos: a) *Dañar*: Consiste en causar detrimento a los datos informáticos, mediante la alteración o supresión de la estructura de datos del *file*, siendo éste un conjunto de registros de datos afines tratados como una unidad de almacenamiento de datos (Vaquero Sánchez, A. y Joyanes Aguilar, L., 1 985, p. 86) que pueden ser fácilmente abiertos a un nivel nativo y aunque no se entienda el lenguaje usado en los registros, la sola modificación o eliminación de líneas de la *file structure*, lo dañan impidiendo que sean correctamente abiertos, prácticamente inservible ; b) *Introducir*, consiste en hacer entrar uno o varios *file* o fichero al sistema informático que podría ser un programa informático, o un dato al file structure, verbigracia, ingresar un dato deliberada e ilegítima a una base de datos, c) *Borrar*, consiste en quitar un fichero o dato que se encuentra en el sistema informático, por ejemplo borrar un registro de una base de datos, d) *Deteriorar*, consiste en hacer pasar el fichero o dato a un Estado, verbigracia, comprimir un archivo de mp3 de 320 kbps a

64 kbps, habrá una pérdida de calidad del audio y reducción del tamaño, pero el contenido es el mismo, también cuantitativamente sigue siendo solo un archivo; e) *Alterar*, consiste en cambiar la esencia del dato, verbigracia en una base de datos, se puede modificar un registro, o recortar un video, en esta mutación altera la estructura de datos, no es la misma, a diferencia del deterioro donde solo se cambia a un Estado malo en el sentido de calidad; f) *Suprimir*, consiste en hacer desaparecer el dato informático, verbigracia eliminar un registro de una base de datos, seleccionar un fichero suprimirlo completamente del disco duro y la g) *Hacer inaccesible*, se trata de procedimiento de hacking que evita el acceso a los datos informáticos, por ejemplo puede ser que se le quiten privilegios de lectura a los ficheros, se cambie su ubicación o nombre para que no sean ubicados por el sistema informático o por el usuario con el fin de solicitarle dinero a cambio de permitir el acceso a los archivos. Es el hacking, mediante virus, la forma más usual de atentar contra los datos, un ejemplo son los ransonware, los troyanos, u otros, que toman el control del sistema de ficheros del sistema operativo, o inyectan líneas de código, o comandos para explotar agujeros de seguridad con la finalidad de sabotear a los usuarios del sistema informático.

14. La conducta de atentar contra los datos informáticos, es de mera actividad (Villavicencio Terreros, F., 2 015), por tanto, se consuma con solo realizar los verbos antes descritos en el tipo penal de manera deliberada e ilegítimamente, sin esperar un resultado posterior, se trata de una afectación directa al objeto del delito, que son la parte lógica de los sistemas informáticos.

15. En este caso no interesa la vulneración de las medidas de seguridad, puesto que se entiende que para efectuar cambios en los datos informáticos, uno debe tener los

permisos de acceso o haberlos vulnerado previamente, en este caso el delito de acceso ilícito sería un delito medio para el sabotaje informático, lo que se debe verificar es el estado de los archivos con un Peritaje Informático, dado que el soporte lógico es muy dinámico en los sistemas informáticos, es decir que los datos informáticos andan cambiando constantemente como parte de la secuencia de comandos o instrucciones propias de los programas informáticos o sistemas informáticos en general, y más si éstos son multiusuario, varios accesos al mismo tiempo a un servidor de base de datos o de contenidos requieren un examen profesional que coadyuve en establecer qué datos y cómo fueron atacados.

16. **Tipo objetivo conglobante. Bien jurídico**: La integridad y disponibilidad de los sistemas informáticos, es el bien jurídico que debe ser ofendido o afectado, ello se desprende del Título 1. del Capítulo II del Convenio sobre la ciberdelincuencia: "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"; dado que el Derecho Penal es sancionador y no constitutivo de bienes jurídicos (Zaffaroni, E. R., 2 016), creemos que este bien jurídico, se funda en el derecho fundamental a la confidencialidad e integridad de sistemas informáticos, desarrollado por el Tribunal Constitucional Federal Alemán en los casos BvR 370/07 - 1 BvR 595/07, como una especie de derivación del derecho fundamental a la personalidad (Persönlichkeitsrecht) (Manssen, G., 2 014, June, p. 39), ubicado en el artículo 22 de la Declaración Universal de Derechos Humanos, el inciso 1 del artículo 2 de la Constitución peruana, por la importancia de las computadoras. Internet, teléfonos móviles y las tecnologías para el desarrollo de la personalidad, puesto que el desarrollo reciente de la tecnología de la información ha hecho que los sistemas de tecnología de la información se vuelvan omnipresentes, y su uso es vital para las vidas de muchos ciudadanos.

17. **Tipo subjetivo:** El *dolo*, es la voluntad realizadora del tipo guiada por el conocimiento de los elementos del tipo objetivo sistemático (Zaffaroni, E. R., 2 009a, p. 108), por ello el agente, que actuó, debe saber y querer dañar, introducir, borrar, deteriorar, alterar, suprimir o hacer inaccesibles los datos informáticos con el *animus hacking*, es decir que deliberada e ilegítimamente atenta contra los datos con el fin de sabotear a los usuarios del sistema informático, es necesario que el agente tenga los conocimientos o habilidades informáticas para realizar estas operaciones, caso contrario el hecho será atípico por ausencia de dolo.

18. El artículo 12 de la Ley 30 096, ha establecido una exención de responsabilidad penal cuando el atentado contra los datos informáticos, se produce con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos; se trata del Penetration Testing (PenTesting), que es una simulación de ataque a un sistema informático, red, o equipos para demostrar vulnerabilidades en caso de un ataque real (Henry, K. M., 2 012, p.12), la cual debe contar con la debida autorización del administrador de los sistemas informáticos, opinamos que ésta al ser parte de todo un procedimiento técnico, por no decir informal, no es necesario contar con una autorización escrita, basta con una orden verbal, opinamos que la actuación sí debe consignarse en algún acta, informe o similar donde se reporten las vulnerabilidades; en este supuesto, el agente actúa con el *animus hacking*, pero lo realiza autorizado por el mismo sujeto pasivo, para encontrar vulnerabilidades, es como una especie de aquiescencia, que podría ubicarse en los términos del contrato o directivas de instalación o mantenimiento de los equipos informáticos, de cualquier manera los problemas que se susciten respecto de ellos, son parte de la esfera privada o administrativa.

19. El artículo 11 de la Ley de Delitos Informáticos, le da mayor reproche penal al agente cuando actúa con el fin de obtener un beneficio económico, esto significa que el objeto del delito, deben ser susceptibles de valoración económica para acreditar el *animus lucrandi*.

20. Concurrencia y participación: Eventualmente, puede producirse una concurrencia con el delito de atentado contra los sistemas informáticos, puesto que al atentar contra los datos estamos indirectamente afectando una parte de los sistemas informáticos que son los archivos que se gestionan por éstos, empero, se debe considerar las definiciones del Convenio de Budapest, para diferenciar los datos de los sistemas y contar siempre con las pericias informáticas para escindir los objetos del delitos afectados.

21. Este tipo penal, admite la coautoría, y la participación de cómplices e instigadores; creemos que los coautores pueden realizar aportes necesarios para la ejecución de la conducta típica, verbigracia, que cada uno de los coautores borre sectores de archivos, se puede distribuir particiones o tipos de archivos, por supuesto que esto demanda determinar el dominio funcional del hecho, y en el caso de la autoría mediata, el dominio de la voluntad del otro.

§ 4. ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS

1. **Genealogía y Derecho Comparado:** El 12 de octubre de 1 984, el Congreso de los Estados Unidos, promulgó la ley "Counterfeit Access Device and Computer Fraud and Abuse Act", que incorporó la §1 030. "Fraud and related activity in connection with computers", ubicado en el Capítulo 47, parte 1, Titulo 18 del Código Federal de los Estados Unidos, esta ley prohibió además del uso no autorizado o el acceso a las computadoras sin autorización, con la enmienda del 2 008, los daños que afecten a un sistema informático utilizado por o para una entidad gubernamental en apoyo de la administración de justicia, la defensa nacional o la seguridad nacional.[12] (Tompkins Jr., J. B. & Mar, L. A., 1 986, p. 460-461; Washingtonpost, 2 003; Kelly, H., 1 977, June 28, p. 36); tales prohibiciones, nacieron en medio de la guerra fría, por tanto el legislador, tenía la intención de cautelar la integridad de la información y los sistemas informáticos donde estaban almacenados.

2. En Alemania, el atentado a la integridad y a los sistemas informáticos, fue sancionado con el *nomen juris* "Computersabotage" (sabotaje informático) ubicado en la § 3 03b del Código Penal Alemán[13]; y el 05 de enero de 1 988, en Francia se

12 §1030. Fraud and related activity in connection with computers(…) Amendments (…) 2008-Subsec. (a)(2)(C). Pub. L. 110–326, §203, struck out "if the conduct involved an interstate or foreign communication" after "computer". "(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)- (…) "(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;".

13 (1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er 1. eine Tat nach § 303a Abs. 1 begeht, 2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder 3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. (2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. (3) Der Versuch ist strafbar. (4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter 1. einen Vermögensverlust großen Ausmaßes herbeiführt, 2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat, 3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der

penalizó la destrucción de datos (Art. 462-4), mediante la Ley 88/19 (Segu.Info, n.d.), que sanciona a quien falsea el funcionamiento de un sistema de tratamiento automático de datos; posteriormente en 1 994, se dicta en el nuevo Código Penal Francés, que sustituyó al Código Napoleónico de 1 810 (Marti, O., 1 994, March 2), este nuevo Código consideró el atentado contra sistemas informáticos en el artículo 323-2[14], sancionando la interferencia o distorsión del funcionamiento de un sistema automatizado de procesamiento de datos.

3. En Chile, la Ley 19 223, publicada el 07 de junio de 1 993, no consideró el atentado contra sistemas informáticos; en España, el Rey Juan Carlos I, el 23 de noviembre de 1 995, sancionó la Ley Orgánica 10/1 995, en el artículo 264 bis del Código Penal Español, que establece: "1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizare o interrumpiera el funcionamiento de un sistema informático ajeno: a) Realizando alguna de las conductas a que se refiere el artículo anterior; b) Introduciendo o transmitiendo datos; o c) Destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración Pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado (...)". En México, el 17 de mayo de 1 999, se publica un Decreto que reforma diversas disposiciones en materia penal, el cual no consideró el atentando a los sistemas informáticos. En el Perú, el 17 de julio del 2 000, se publicó la

Bundesrepublik Deutschland beeinträchtigt. (5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

14 Article 323-2 Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4 Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

Ley 27 309 "Ley que incorpora los delitos informáticos al Código Penal", que contempla el daño de datos y daño de sistemas informáticos en el artículo 207-B, sin *nomen juris,* en ninguno de los Proyectos de Ley se hizo mención de ella, tampoco en los debates[15], por lo que la Doctrina no es uniforme en su denominación (Reyna Alfaro, L. M, 2 002, p. 260; Salinas Siccha, R., 2 008, p.1206, Peña Cabrera Freyre, A. R., 2 015, p. 729; Gálvez Villegas, T. A., Delgado Tovar, W. J, 2 011, 1 217) los juristas lo denominaron como "Sabotaje Informático", "Alteración, daños, destrucción de la información y la base de datos", la fórmula legal decía, "El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma, con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.", con la agravante del artículo 207-C "En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional".

4. En Ecuador, con la Reforma del 2 002 al Código Penal Ecuatoriano, mediante la Ley 2 002-67, se hizo una reforma penal que no consideró el daño al sistema informático, y se ubica en el artículo 232 del Código Orgánico Integral de Ecuador (2 014), cuyo texto señala "La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes

15 Fueron tres los Proyectos de Ley, con los números 0507/99, 05132/99, 05326/99, presentados en el año 1 999. Los debates se realizaron el 03 mayo y 21 de junio de 1 999.

lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.”.

5. En Argentina, en el año 2 008, el art. 5 de la Ley 26 388, incorporó al Código Penal Argentino, diversos artículos sobre Delitos Informáticos, entre ellos el artículo 183, que reprime al que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. En nuestro país, el 22 de octubre de 2 013, se publicó en el Diario Oficial el Peruano, la Ley de Delitos Informáticos: Ley 30 096, con Fe de Erratas publicado al día siguiente en una edición extraordinaria del mencionado Diario, el atentado a la integridad de los sistemas informáticos fue ubicado en el artículo 4 de la mencionada Ley, tuvo el siguiente texto: “El que, a través de las Tecnologías de la Información y de la Comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a éste, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa”.

6. La adopción o la compatibilidad con los criterios del Convenio de Budapest “Convenio sobre la Ciberdelincuencia” (Council of Europe, 2 001), fue uno de los fundamentos de los Proyectos de Ley con los números 03105/2 013-CR, 03048/2 013-CR, 03017/2 013-CR 2 999/2 013-CR, 2991/2 013-CR y habiéndose tomado como texto base, la fórmula legal del atentado a la integridad de datos provino del citado Convenio traducido al español a la Ley 30 171 que modificó la Ley 30 096, para comprobar ello, revisemos el texto del Convenio, que dice:

Artículo 5. Interferencia en el sistema

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

El artículo 4 de la Ley de Delitos Informáticos (Ley 30 096), cuyo texto dice:

Artículo 4. Atentado a la integridad de sistemas informáticos

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a éste, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

7. **Balance histórico:** a) Sobre la naturaleza del delito, el atentado a la integridad de sistemas informáticos, es un tipo que surge como una conducta derivada del espionaje contra el Estado, y transita por diversos países hasta convertirse en un Delito Informático que atañe a sujetos comunes, no siendo siempre el Estado y las empresas del sujeto pasivo; b) El contenido del injusto del hecho típico, nació como un tipo de baja gravedad, y comparativamente con la penalidad en países de Latinoamérica (Riquert, M. A., 2 014, p. 232), observamos que hay una tendencia a incrementar el máximo del marco abstracto de la pena, bajo el argumento que la comisión y los daños

son equiparables a los delitos comunes, en el caso del atentado contra los sistemas informáticos, equivaldría a que un delincuente ingrese a una casa y queme o destruya un taller de carpintería; c) Requisitos típicos más notorios, que el sujeto activo debe atentar contra la integridad o funcionamiento de los sistemas informáticos que comprende equipos de cómputo y redes que sirven para automatizar la información, lo que se conoce como TIC, por supuesto que nos referimos al aspecto material de éste, es decir solo el soporte físico, queda fuera de la prohibición típica del software que es parte de los datos informáticos.

8. El tipo nació en una coyuntura bélica, en la que los Gobiernos debían proteger los secretos de Estado y de la empresa, tributarios necesarios para financiar la carrera armamentista, en ese contexto, tenía un sentido de protección contra el espionaje y sabotaje informático, posteriormente, cuando la comunicación por ordenadores se masificó, el tipo, cobró un sentido de protección contra todos los sistemas informáticos públicos y privados de cualquier persona.

9. En algunos países, el tipo penal era parte de una misma fórmula legal de Sabotaje Informático, que comprendía tanto la interferencia de datos como la interferencia de sistemas informáticos que en el Convenio sobre Cibercriminalidad, fue tratado de forma individual. En el Perú, el atentado contra datos informáticos aparece como una especie de sabotaje informático con la Ley 27 309, que incorporó los Delitos Informáticos al Código Penal peruano, la misma, como le mencionamos en líneas arriba, que eclosiona en medio de un Gobierno dictatorial y corrupto de Fujimori y Montesinos (López Martínez, H., 2 011, p. 68, 72; Palacios Rodriguez, R., 2 014, p. 245-247, 254), el ex presidente Alberto Fujimori Fujimori, bajo esa línea autoritaria,

mediante una observación a la Autógrafa de la citada Ley, propuso regular como agravante y con mayor severidad, cuando el sujeto pasivo sea una organización de defensa nacional, seguridad interior, inteligencia, o cuando se afecte la seguridad de la Nación, asimismo cuando el agente en razón de su cargo o puesto de trabajo tuviere acceso a información clasificada o privilegiada, y se aprovecha para cometer el delito. (Fujimori Fujimori, A. 2 000, May 30), propuesta que emergió como reflejo de una ideología heredada de la guerra fría, que con el artículo 207-C permeó en la legislación peruana, la que estableció hasta antes del año 2 013, que en los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional; y después del año 2 013, lo sucedido -en esta política criminal- el artículo 11 de la Ley de Delitos Informáticos, cuando le da mayor reproche penal al agente del delito al comprometer fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

10. **Tipo objetivo. Los sujetos:** El *sujeto activo*, es cualquier persona natural, no se exige alguna condición especial o relación con el sujeto pasivo y el sistema informático; en cuanto al *sujeto pasivo*, éste puede ser una persona natural o jurídica. La Doctrina nacional, sostiene que el sujeto activo debe tener conocimientos o habilidades de informática necesarios para la acción típica (Reyna Alfaro, L. M, 2 002, p. 261; Salinas Siccha, R., 2 008, p.1 210, Peña Cabrera Freyre, A. R., 2 015, p. 729-730; Gálvez Villegas, T. A., Delgado Tovar, W. J., 2 011, p. 1 217).

11. Originariamente, el agente activo solo era un hacker, el delincuente de cuello blanco, y el pasivo, el Estado y la Empresa, con la comercialización de las TIC, el ámbito de prohibición se amplió, ocasionando un cambio cualitativo en los sujetos en el Convenio de Budapest, que influyó en el legislador peruano.

12. El artículo 11 de la Ley de Delitos Informáticos, le da mayor reproche penal al agente cuando es integrante de una organización criminal, abusa de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

13. Tipo objetivo sistemático. La exteriorización de la acción: Según el artículo 1, literal "a" del Convenio de Budapest, se entenderá por «Sistema Informático» todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa; el tipo prohíbe que de manera intencionada o deliberada e indebida o contra el Ordenamiento Jurídico, se inutilice total o parcialmente los sistemas informáticos, hacerlas inaccesibles o entorpecer su funcionamiento y prestación de servicios, ahora bien, examinemos las conductas de manera sintética: a) Inutilice, total o parcialmente, un sistema informático, se refiere a restarle aptitud de operatividad al sistema informático, dañándolo o destruyéndolo físicamente, verbigracia, disparar contra un rack de servidores de base de datos, omitiendo otros racks y cableado (de forma parcial); b) Impide el acceso al sistema informático, consiste en imposibilitar el acceso físico a los sistemas informáticos, por ejemplo, dañar las chapas de seguridad de las puertas de acceso al data center donde se encuentran un montón de racks de servidores con gabinetes sin puertas, es decir que no

hay más seguridad que las puertas del ambiente, esto con el fin de evitar que el personal de informática opere los dispositivos; c) Entorpece o imposibilita su funcionamiento, se refiere a obstaculizar el funcionamiento de los dispositivos que conforman el sistema informático, verbigracia, cortar el suministro eléctrico, o retirar un disco duro que contiene el sistema operativo (SO) de uno de los servidores, y d) Entorpece o imposibilita la prestación de sus servicios, consiste en obstaculizar el uso del sistema informático en pleno funcionamiento por parte de los usuarios, por ejemplo bloquear las señalas del servicio de Internet inalámbrico (Wifi) o Bluethoot, con la técnica del *Jamming*.

14. La conducta de atentar contra los sistemas informáticos, es de resultado (Villavicencio Terreros, F., 2 015, p. 13), por tanto, se consuma al concluir el plan criminal, no basta realizar los verbos antes descritos en el tipo penal de manera deliberada e ilegítimamente, por lo que debe acreditar el resultado posterior, se trata de una afectación al objeto del delito, que es la parte física de los sistemas informáticos.

15. Puede tratarse de un delito medio para el atentado contra los datos informáticos, o acceso ilícito, de todos modos, para acreditar el delito se requiere un Peritaje Informático, para determinar si la afectación fue total o parcial, estableciendo la totalidad del sistema informático, puede tratarse de uno complejo, y establecer si la conducta fue idónea para interferir el funcionamiento o prestación de servicios del sistema informático.

16. **Tipo objetivo conglobante. Bien jurídico**: La integridad y disponibilidad de los sistemas informáticos, es el bien jurídico que debe ser ofendido o afectado, ello

se desprende del Título 1. del Capítulo II del Convenio sobre la ciberdelincuencia: "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"; dado que el Derecho Penal, es sancionador y no constitutivo de bienes jurídicos (Zaffaroni, E. R., 2 016), creemos que este bien jurídico, se funda en el Derecho fundamental a la confidencialidad e integridad de sistemas informáticos, desarrollado por el Tribunal Constitucional Federal Alemán en los casos BvR 370/07 - 1 BvR 595/07, como una especie de derivación del derecho fundamental a la personalidad (Persönlichkeitsrecht) (Manssen, G., 2 014, June, p. 39), ubicado en el artículo 22 de la Declaración Universal de Derechos Humanos, el inciso 1 del artículo 2 de la Constitución peruana, por la importancia de las computadoras. Internet, teléfonos móviles y las tecnologías para el desarrollo de la personalidad, puesto que el desarrollo reciente de la tecnología de la información ha hecho que los sistemas de tecnología de la información se vuelvan omnipresentes, y su uso es vital para las vidas de muchos ciudadanos.

17. **Tipo subjetivo:** El *dolo*, es la voluntad realizadora del tipo guiada por el conocimiento de los elementos del tipo objetivo sistemático (Zaffaroni, E. R., 2 009a, p. 108), por ello el agente, que actúa, debe saber y querer inutilizar, total o parcialmente, un sistema informático, impedir el acceso a éste, entorpecer o imposibilitar su funcionamiento o la prestación de sus servicios con el *animus hacking*, es decir que deliberada e ilegítimamente atenta contra los dispositivos y redes de conexión con el fin de sabotear a los usuarios del sistema informático, es necesario que el agente tenga los conocimientos o habilidades informáticas para realizar estas operaciones, caso contrario el hecho será atípico por ausencia de dolo, por ejemplo, no sería típico la conducta de un delincuente que sin conocimientos en informática entra en un data center y roba

cualquier equipo del sistema informático, se trataría de un delito contra el patrimonio, pero no un delito informático, pues, la del tipo objetivo se realiza pero hay el *animus hacker*, es decir que carece de motivación, no sabe el cómo y para qué inutilizar el sistema informático de manera idónea, sabiendo que con ello impedirá el funcionamiento o prestación de servicios, por ejemplo, un hacker que quiere inutilizar un servidor de página web, estando frente al rack, no dispararía solo al teclado o al monitor; sino directo al CPU del servidor porque sabe que ahí está el núcleo central de todo el aparato, el disco duro, las memorias RAM, las tarjetas, etc.

18. El artículo 12 de la Ley 30 096, ha establecido una exención de responsabilidad penal cuando el atentado contra los sistemas informáticos, se produce con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos; se trata del Penetration Testing (PenTesting), que es una simulación de ataque a un sistema informático, red, o equipos para demostrar vulnerabilidades en caso de un ataque real (Henry, K. M., 2 012, p.12), la cual debe contar con la debida autorización del administrador de los sistemas informáticos, opinamos que ésta al ser parte de todo un procedimiento técnico, por no decir informal, no es necesario contar con una autorización escrita, basta con una orden verbal, opinamos que la actuación sí debe consignarse en algún acta, informe o similar donde se reporte las vulnerabilidades; en este supuesto, el agente actúa con el *animus hacking*, pero lo realiza autorizado por el mismo sujeto pasivo, para encontrar vulnerabilidades, es como una especie de aquiescencia, que podría ubicarse en los términos del contrato o directivas de instalación o mantenimiento de los equipos informáticos, de cualquier manera los problemas que se susciten respecto de ellos, son parte de la esfera privada o administrativa.

19. El artículo 11 de la Ley de Delitos Informáticos, le da mayor reproche penal al agente cuando actúa con el fin de obtener un beneficio económico, esto significa que el objeto del delito, deben ser susceptibles de valoración económica para acreditar el *animus lucrandi*.

20.Concurrencia y participación: Eventualmente, puede producirse una concurrencia con el delito de atentado contra los datos informáticos, puesto que al atentar contra los sistemas informáticos, estamos indirectamente afectando los datos almacenados en los sistemas informáticos, empero, se debe considerar las definiciones del Convenio de Budapest y la finalidad del agente, para diferenciar los datos de los sistemas y contar siempre con las pericias informáticas para escindir los objetos del delitos afectados.

21.Este tipo penal, admite la coautoría, y la participación de cómplices e instigadores; creemos que los coautores pueden realizar aportes necesarios para la ejecución de la conducta típica, verbigracia, que cada uno de los coautores atenta con varios gabinetes de servidores, por supuesto que esto demanda determinar el dominio funcional del hecho, y en el caso de la autoría mediata, el dominio de la voluntad del otro.

§ 5. PROPOSICIONES A NIÑOS, NIÑAS Y ADOLESCENTES CON FINES SEXUALES POR MEDIOS TECNOLÓGICOS

1. **Genealogía:** El artículo 2 de la Ley 27 459, publicada el 26 de mayo de 2 001, incorporó al Código Penal, el artículo 183-A, con el *nomen juris* "Pornografía infantil", posteriormente fue modificado por el artículo 1 de la Ley 28 251, publicada el 08 de junio del 2 004, la que fue innovada incluyéndose como vía típica el Internet a propuesta del Dictamen de la Comisión de la Mujer y Desarrollo Social del Congreso de la República del Perú (2 003, December 4, p. 10), hasta que fue modificado por la Cuarta Disposición Complementaria Modificatoria de la Ley 30 096, publicada el 22 octubre del 2 013, en la que se reemplazó el término *Internet*, por Tecnologías de la Información y de la Comunicación ubicándola como una agravante, finalmente el artículo 5 de la Ley 30 171, publicada el 10 marzo del 2 014, incorporó el artículo 183-B, con el *nomen juris* "Proposiciones sexuales a niños, niñas y adolescentes" con el siguiente texto:

> El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36.

Notamos que la redacción prescinde de las Tecnologías de la Información y Comunicación, a diferencia de la fórmula legal contenida en el artículo 5 de la Ley de Delitos Informáticos.

2. El 17 de julio del 2 000, se publicó la Ley 27 309 "Ley que incorpora los Delitos Informáticos al Código Penal", la cual no contempló la pornografía infantil por medio de las TIC, fue el interés del legislador por la compatibilidad con los criterios del Convenio de Budapest. "Convenio sobre la Ciberdelincuencia" (Council of Europe, 2 001), en hacer que el siguiente texto del Convenio de Budapest sea tomado como base para la Ley de Delitos Informáticos en el Perú.

Artículo 9. Delitos relacionados con la Pornografía Infantil."

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b) La oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c) La difusión o transmisión de pornografía infantil por medio de un sistema informático,

d) La adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e) La posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

(...)

4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

El texto fue recibido parcialmente en la Ley de Delitos Informáticos (Ley 30 096), con la modificatoria de la Ley 30 171, publicada el 10 marzo del 2 014, cuyo texto dice:

> **Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos**
>
> El que a través de Internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.
>
> Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

3. **Balance histórico:** a) Sobre la naturaleza del delito de ciberacoso sexual, también llamado grooming o child grooming (Franco Gonzales, C.A., 2 015, December), consistente en la propuesta sexual a niños, niñas y adolescentes con fines sexuales, es un tipo que surge como una conducta desligada de la tecnología, con el tiempo admitió como medio al Internet, y la TIC, por ello es un delito computacional; b) El contenido del injusto del hecho típico, nació como un tipo de baja gravedad, fue incrementándose y se mantiene y la pena es menor que un tipo común, puesto que la acción es de menor reproche, dado que no están consideradas todas las acciones del Convenio sobre ciberciminalidad; c) Requisitos típicos más notorios, que el sujeto activo debe atentar contra la indemnidad y libertad sexual mediante el Internet.

4. **Tipo objetivo. Los sujetos:** El *sujeto activo*, es cualquier persona natural, en cuanto al *sujeto pasivo*, es una persona natural menor de 14 años, y para la agravante entre 18 y 14años. Originariamente, el sujeto pasivo, no estaba considerado, salvo en la agravante, pero solo el menor de 14 años, y en el Convenio de Budapest, no se precisa la edad del menor de edad, por lo que queda al legislador de cada país completar la fórmula legal, observando la Convención sobre los Derechos del Niño (Art. 19) y el Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (Art. 3).

5. Puede darse el caso que el agente sea un menor, en este supuesto, asunto que será tratado por el derecho penal de menores, esto podría producirse en el marco del ciberacoso o cyberbullying, que es una forma de violencia entre pares que implica el uso de las TIC –teléfonos móviles, Internet, videojuegos– para acosar, amenazar o intimidar deliberadamente a alguien (Save The Children, 2 013, p. 10).

6. El artículo 11 de la Ley de Delitos Informáticos, le da mayor reproche penal al agente cuando es integrante de una organización criminal, abusa de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

7. Tipo objetivo sistemático. La exteriorización de la acción: Según el artículo 9, inciso 2 y 3 del Convenio de Budapest, se entenderá por «Pornografía Infantil» a todo material pornográfico que contenga la representación visual de: a) Un menor comportándose de una forma sexualmente explícita; b) Una persona que parezca un menor comportándose de una forma sexualmente explícita; c) Imágenes realistas que

representen a un menor comportándose de una forma sexualmente explícita. La conducta sancionada consiste en contactar o comunicarse usando el Internet u otro medio análogo, como llamadas de teléfono, mensajes de texto para contactar con un menor de 14 años parar pedir u obtener de él material pornográfico, o para solicitarle llevar a cabo actividades sexuales con él, con la agravante si la víctima tiene entre 14 y 18 años de edad y media engaño, que según la Doctrina se trata de un instrumento para invalidar la voluntad de la víctima (Peña- Cabrera Freyre, A. R., 2 015, p. 291).

8. La conducta de contacto, es de resultado y no de mera actividad como afirma la Doctrina peruana (Villavicencio Terreros, F., 2 015, p. 16; Peña-Cabrera Freyre, A. R., 2 015, p. 292), por tanto se consuma cuando conforme al plan criminal, hay respuesta a la comunicación, sea positiva o negativa de parte del sujeto pasivo, puesto que no se trata de un contacto unilateral, es necesario la interacción, en su defecto, la acción quedaría en grado de tentativa tanto en la intención de solicitar u obtener material pornográfico o pedir actividad sexual, todo a través del Internet, que podría ser por el Facebook, Twitter, correo electrónico, mensajería por Internet móvil como el Whatsapp, Telegram, etc.

9. La UNODC, define algunas formas de comisión, o digamos de contacto con menores, como (a) El sexting, es el envío y/o recepción de contenido sexual a través de medios electrónicos (redes sociales, e-mail, teléfono móvil), y (b) Sextortion, es una forma de extorsión en la que se chantajea a una persona por medio de una imagen o video de sí misma desnuda, que puede ser compartida a través de Internet o mensajes.

10. **Tipo objetivo conglobante. Bien jurídico**: Para el primer párrafo del tipo penal, es la *indemnidad sexual*, entendida como la preservación de la sexualidad de una persona cuando no está en condiciones de decidir sobre su actividad sexual (Corte Suprema de Justicia. Primera Sala Penal Transitoria, R.N. 4 403-2 008), de este modo, se brinda amparo a la dignidad de los niños, niñas y adolescentes en el mundo digital, frente a este nuevo fenómeno tecnológico, que es descrito por el Santo Padre Francisco, con las siguientes palabras en un congreso sobre "La dignidad del menor en el mundo digital":

> En la red se están propagando fenómenos extremadamente peligrosos: La difusión de imágenes pornográficas cada vez más extremas, porque con la adicción se eleva el umbral de la estimulación; el creciente fenómeno del sexting entre chicos y chicas que utilizan las redes sociales; la intimidación que se da cada vez más en la red y representa una auténtica violencia moral y física contra la dignidad de los demás jóvenes; la sextortion; la captación a través de la red de menores con fines sexuales es ya un hecho del que hablan continuamente las noticias; hasta llegar a los crímenes más graves y estremecedores de la organización online del tráfico de personas, la prostitución, incluso de la preparación y la visión en directo de violaciones y violencia contra menores cometidos en otras partes del mundo. Por lo tanto, la red tiene su lado oscuro y regiones oscuras (la dark net) donde el mal consigue actuar y expandirse de manera siempre nueva y cada vez con más eficacia, extensión y capilaridad. La antigua difusión de la pornografía a través de medios impresos era un fenómeno de pequeñas dimensiones comparado con lo que está sucediendo hoy en día, de una manera cada vez más creciente y rápida, a través de la red (2 017).

Ciertamente, el *Internet*, es un medio de propagación masiva de información, que puede ser fácilmente usado para establecer comunicación con los menores, y para la difusión de pornografía, y no solo en la Dark Net; sino que en cualquier sitio web o en las redes sociales, por el egoísmo carnal del ser humano, y el interés económico de quienes las publican sin filtros ni medidas de seguridad, con tal de obtener dinero por la publicidad que se presenta en estos sitios de Internet.

11.En el supuesto de menores entre 14 y 18 años (segundo párrafo), considerando el derecho al desarrollo de la personalidad (Cons. Art. 2.1, y la STC 00008-2 012-PI/TC), es menester precisar que la afectación del bien jurídico ***libertad sexual*** (Franco Gonzales, C. A., 2015, p. 261) genera un pragma conflictivo, solo si se trata de comunicaciones sin consentimiento, es decir, que el agente persiste en sus solicitudes, no obstante, que el sujeto pasivo haya expresado su negativa a recibir estas comunicaciones, de lo contrario, si ambos sujetos están de acuerdo en dialogar de manera expresa no tácita sobre contenido sexual, verbigracia una pareja de enamorados, nos parece conveniente frenar al poder punitivo, siempre atendiendo a las particularidades de cada caso concreto que nos conduzcan a concluir que existió tal consentimiento dentro de la tipicidad conglobante.

12. **Tipo subjetivo:** El *dolo*, es la voluntad realizadora del tipo guiada por el conocimiento de los elementos del tipo objetivo sistemático (Zaffaroni, E. R., 2 009a, p. 108), por ello el agente, que actúa, debe saber y querer cada de uno de los elementos del tipo objetivo sistemático, por ejemplo la edad de los niños, niñas y adolescentes, y tener claro la finalidad "el para" el cual constituye un elemento de trascendencia interna,

el propósito, más allá de hacer contacto, es pedir material pornográfico o actividades sexuales.

13. El artículo 11 de la Ley de Delitos Informáticos, le da mayor reproche penal al agente cuando actúa con el fin de obtener un beneficio económico, esto significa que el objeto del delito, deben ser susceptibles de valoración económica para acreditar el *animus lucrandi*.

14. Concurrencia y participación: Es posible que se presente un concurso real con delitos de pornografía infantil y violación sexual (181-A, 182-A, 183, 183-A), el child grooming, se diferencia de ellos, porque éste constituye la fase previa de la consumación de los delitos mencionados (Franco Gonzales, C. A., 2 015, p. 259), además que la finalidad del autor es tan solo "contactar" mediante Internet.

15.Este tipo penal, admite la coautoría, y la participación de cómplices e instigadores; creemos que los coautores pueden realizar aportes necesarios para la ejecución de la conducta típica, verbigracia, que cada uno de los coautores establezca contacto sobre una misma finalidad dentro de un único plan criminal que la beneficiaría a los coautores, esto demanda determinar el dominio funcional del hecho, y en el caso de la autoría mediata, el dominio de la voluntad del otro.

§ 6. INTERCEPTACIÓN DE DATOS INFORMÁTICOS

1. **Genealogía y Derecho Comparado:** La interceptación de datos, al igual que otras figuras que se examinaron líneas arriba proviene del delito de acceso ilícito, que fue promulgado el 12 de octubre del 1 984, por el Congreso de los Estados Unidos, con la ley "Counterfeit Access Device and Computer Fraud and Abuse Act", en ella se prohibió el acceso o todo tipo de forma de divulgación de información para cautelar la seguridad nacional y el secreto empresarial, que en la guerra fría trabajaban de la mano, puesto que la empresa fue tributario de la guerra armamentista; y la preocupación por la interceptación que ya venía desde las guerras mundiales, como la tarea emprendida por Alan Turing en descifrar el Código Engima, máquina nazi de cifrado y descifrado de mensajes (Leavitt, D., 2 006, p. 11), que para ese entonces se hacía a mano, por así decirlo, sin la intervención del ordenador o computadora.

2. En nuestro país, en la Ley de Delitos Informáticos 30 096, la interceptación de datos informáticos está ubicado en el artículo7 de la mencionada Ley, y por el afán de compatibilidad con los criterios del Convenio de Budapest "Convenio sobre la Ciberdelincuencia"se promulgó la Ley 30 171 que modificó la Ley 30 096, y tomó base el siguiente texto del Convenio, con excepción de las agravantes:

> Artículo 3. Interceptación ilícita
>
> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos

datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Con la modificatoria de la Ley 30 171, publicada el 10 marzo del 2 014, actualmente el texto dice:

Artículo 7. Interceptación de datos informáticos

El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años, cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27 806, Ley de Transparencia y Acceso a la Información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

3. **Balance histórico:** a) Sobre la naturaleza del delito de interceptación de datos informáticos, es un tipo que surge a partir del delito de acceso ilícito; b) El contenido

del injusto del hecho típico, nació como un tipo de baja gravedad, fue incrementándose cuando se trata de información confidencial que afecta la defensa, seguridad y soberanía nacional; c) Requisitos típicos más notorios, que la información transmitida debe provenir de un sistema informático.

4. **Tipo objetivo. Los sujetos:** El *sujeto activo*, es cualquier persona natural, en cuanto al *sujeto pasivo*, es una persona natural, también el Estado cuando éste es el titular de la información que ha sido recopilada.

5. Si el agente comete el delito como integrante de una organización criminal, la consecuencia jurídica se incrementa hasta en un tercio por encima del máximo legal.

6. Tipo objetivo sistemático. La exteriorización de la acción: Según el artículo 1 del Convenio de Budapest, se entenderá por «Sistema Informático» todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa, por «Datos Informáticos» se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función y por «Datos Sobre el Tráfico» se entenderá cualesquiera de datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente; el tipo prohíbe que de manera intencionada o deliberada e indebida o contra el Ordenamiento Jurídico, se intercepte

datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, lo que en otras palabras consiste en apoderarse de información digital que proviene y va a un sistema informático público o privado, que se transmite de manera alámbrica o inalámbrica, el traslado de datos binarios, analógicos, codificado o no, puede ser susceptible de apoderamiento por parte de herramientas de tecnologías que con las que se equipan los hacker (craker); en cuanto a la información que circula dentro del sistema informático, es posible que ésta se realice mediante virus informáticos, como un malware recolector de información como el Regin, que se implanta en el Microsoft Windows, el cual según la prensa indican que fue usado por agencias de inteligencia estadounidense y británica para atacar a la Unión Europea (Marquis-Boire, M; Guarnieri, C.; Gallagher, R., 2 014, November 24), hecho que pudo haber capturado información secreta, reservada o confidencial, que comprometa la defensa, seguridad o soberanía nacionales, definición y presupuestos legales que deben extraer de la Ley 27 806: Ley de Transparencia y Acceso a la Información Pública, de lo que inferimos que se trata de un tipo objetivo abierto.

7. La conducta de interceptar los datos, es de resultado y no de mera actividad como afirma la Doctrina peruana (Villavicencio Terreros, F., 2 015, p. 17), por tanto se consuma cuando conforme al plan criminal, primero se inicia la ejecución de recopilación de datos y como resultado se obtiene los datos informáticos de forma íntegra o completa, de lo contrario contaríamos con información corrupta o dañada, lo cual le resta de funcionalidad o utilidad, quedando la conducta en grado de tentativa, esto en consideración a la realidad que el traslado digital de información es muy estricto

en su completitud, aspecto que le dota plena funcionalidad dicho de otro modo, que puede ser leído y reproducido, requisito necesario para su consumación, la que debe ser objeto de Pericia Informática, puesto que hay ficheros o datos parciales que pueden cobrar cierta individualidad al ser escindidos.

8. **Tipo objetivo conglobante. Bien jurídico**: La disponibilidad de datos de los sistemas informáticos, es el bien jurídico que debe ser ofendido o afectado, ello se desprende del Título 1. del Capítulo II del Convenio sobre la ciberdelincuencia: "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"; dado que el Derecho Penal es sancionador y no constitutivo de bienes jurídicos (Zaffaroni, E. R., 2 016), creemos que este bien jurídico, se funda en el derecho fundamental a la confidencialidad e integridad de sistemas informáticos, desarrollado por el Tribunal Constitucional Federal Alemán en los casos BvR 370/07 - 1 BvR 595/07, como una especie de derivación del derecho fundamental a la personalidad (Persönlichkeitsrecht) (Manssen, G., 2 014, June, p. 39), ubicado en el artículo 22 de la Declaración Universal de Derechos Humanos, el inciso 1 del artículo 2 de la Constitución peruana, por la importancia de las computadoras, Internet, teléfonos móviles y las tecnologías para el desarrollo de la personalidad, puesto que el desarrollo reciente de la tecnología de la información ha hecho que los sistemas de tecnología de la información se vuelvan omnipresentes, y su uso es vital para las vidas de muchos ciudadanos.

9. **Tipo subjetivo:** El *dolo,* es la voluntad realizadora del tipo guiada por el conocimiento de los elementos del tipo objetivo sistemático (Zaffaroni, E. R., 2 009a, p. 108), por ello el agente, que actúa, debe saber y querer cada de uno de los elementos

del tipo objetivo sistemático, por ejemplo que se trata de datos informáticos confidenciales, de carácter público o privado, etc., en aras de conseguir una imputación concreta respetuoso del Principio de Legalidad, ello implica que el agente tenga habilidades informáticas acreditadas, suponer que ya los tiene, incrementaría enormemente la situación de vulnerabilidad de los ciudadanos frente al poder punitivo, de modo que el solo usar las TIC, nos haría delincuentes en potencia.

10. El artículo 11 de la Ley de Delitos Informáticos, le dé mayor reproche penal al agente cuando actúa con el fin de obtener un beneficio económico, esto significa que el objeto del delito, deben ser susceptibles de valoración económica para acreditar el *animus lucrandi*.

11.Concurrencia y participación: Es posible que se presente un concurso aparente con la segunda modalidad del artículo 162 del Código Penal peruano, referido a la escucha de una conversación telefónica, en este caso, debemos enfocarnos en la definición de sistema informático, excluyendo del mismo a la función de teléfono, entendido como conjunto de aparatos e hilos conductores con los cuales se transmite a distancia la palabra y toda clase de sonidos por la acción de la electricidad (Real Academia Española, 2 014), sostenemos que se refiere a la función de teléfono, de manera restrictiva, en razón que son muchos los aparatos de comunicación que cumplen múltiples funciones de comunicación entre ellas las de teléfono, que vienen a ser también sistemas informáticos, pero el artículo en mención por legalidad estricta solo hace mención al teléfono, y no a la Tablet o Smartphone en general, dado que estos, muy aparte de contar con un aplicativo de llamadas por la red telefónica como el GSM, éstas cuentan con Whatsapp, Facebook Messenger, Telegram, Skype, otras aplicaciones

que operan con Internet móvil o Wifi, en sí, la arquitectura de comunicaciones es distinta, se trata de sistemas informáticos de comunicaciones más complejas que emiten y reciben datos informáticos, por lo que son contempladas por el tipo penal de interceptación de datos informáticos.

12.Este tipo penal, admite la coautoría, y la participación de cómplices e instigadores; creemos que los coautores pueden realizar aportes necesarios para la ejecución de la conducta típica, verbigracia, que cada uno de los coautores opere cada una de las herramientas del kit de interceptación con las que cuentas los delincuentes informáticos sobre una misma finalidad dentro de un único plan criminal que los beneficiaría a los coautores, esto demanda determinar el dominio funcional del hecho, y en el caso de la autoría mediata, el dominio de la voluntad del otro.

§ 7. FRAUDE INFORMÁTICO

1. **Genealogía y Derecho Comparado:** El fraude informático, al igual que otras figuras que se examinaron líneas arriba proviene del delito de acceso ilícito, que fue promulgado el 12 de octubre de 1 984, por el Congreso de los Estados Unidos, con la ley "Counterfeit Access Device and Computer Fraud and Abuse Act", en ella se prohibió el acceso o todo tipo de forma de divulgación de información que además de sancionar los perjuicios económicos, protegía la seguridad nacional y el secreto empresarial, que en la guerra fría trabajaban de la mano, puesto que, como se dijo, la empresa fue tributario de la guerra armamentista; y la preocupación por el valor de la información fue siempre importante para el centro del mundo.

2. En nuestro país, en la ley de Delitos Informáticos Ley 30 096, el Fraude Informático está ubicado en el artículo 8 de la mencionada ley, y por el afán de compatibilidad con los criterios del Convenio de Budapest "Convenio sobre la Ciberdelincuencia"se promulgó la Ley 30 171 que modifico la Ley 30 096, y tomó como base el siguiente texto del Convenio:

> Artículo 8. Fraude informático
>
> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:
>
> a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;
>
> b) Cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Con la modificatoria de la Ley 30 171, publicada el 10 marzo del 2 014, actualmente el texto dice:

> **Artículo 8. Fraude Informático**
>
> El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático,

será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

3. **Balance histórico:** a) Sobre la naturaleza del Delito de Fraude Informático, es un tipo que surge a partir del delito de acceso ilícito; b) El contenido del injusto del hecho típico, nació como un tipo de acceso ilícito de baja gravedad, fue incrementándose cuando se trata de perjuicio patrimonial; c) Requisitos típicos más notorios, que el fraude sea para provecho ilícito.

4. **Tipo objetivo. Los sujetos:** El *sujeto activo*, es cualquier persona natural, en cuanto al *sujeto pasivo*, es una persona natural o jurídica, también el Estado cuando éste es el titular del patrimonio.

5. El artículo 11 de la Ley de Delitos Informáticos, le dé mayor reproche penal al agente cuando es integrante de una organización criminal, abusa de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

6. Tipo objetivo sistemático. La exteriorización de la acción: Según el artículo 1 del Convenio de Budapest, se entenderá por «Sistema Informático» todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa, por «Datos Informáticos» se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el

tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función y por «Datos Sobre el Tráfico» se entenderá cualesquiera de datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente; el tipo prohíbe que de manera intencionada o deliberada e indebida o contra el Ordenamiento Jurídico, se procure para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño (proyecto de aplicativos, programas informáticos o dispositivos), introducción (hacer entrar o instalar programas informáticos o dispositivos), alteración (modificar la estructura lógica para evitar o producir otros resultados), borrado (eliminar, quitar o desparecer programas informáticos que son parte del sistema informático), supresión (cesar, o hacer desaparecer dispositivos del sistema informático), clonación de datos informáticos (hacer clones, producir datos idénticos a otros contenidos en soporte físico) o cualquier interferencia (disminución o anulación del funcionamiento) o manipulación en el funcionamiento de un sistema informático (operar o manejar el sistema informático), con la agravante si se afecta el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

7. La conducta de interceptar los datos, es de resultado (Villavicencio Terreros, F., 2 015, p. 19), por tanto se consuma cuando conforme al plan criminal, se ocasiona el perjuicio patrimonial a tercero con el aprovechamiento ilícito para sí o para otro, con la realización de cada uno de los verbos típicos del tipo penal, por ejemplo el caso del hacker ruso Stanislav Lísov quien cometió con fraude con el malware “NeverQuest”, que es troyano bancario que afectó a instituciones financieras por la suma de 855 mil dólares americanos (El Mundo, 2 017, July 16).

8. **Tipo objetivo conglobante. Bien jurídico**: De la redacción del tipo penal se infiere que el bien jurídico corresponde al patrimonio, porque luego de las operaciones fraudulentas realizadas por el agente, se ocasiona un perjuicio económico, puesto que el autor obtiene un desplazamiento económico a su favor atentando contra los datos y sistemas informáticos que contienen información, verbigracia, el agente debe saber que está clonando una tarjeta de débito y el querer con ello ocasionar un perjuicio económico al titular de la cuenta, reiterando todo el dinero.

9. **Tipo subjetivo:** El *dolo,* es la voluntad realizadora del tipo guiada por el conocimiento de los elementos del tipo objetivo sistemático (Zaffaroni, E. R., 2 009a, p. 108), por ello el agente, que actúa, debe saber y querer cada de uno de los elementos del tipo objetivo sistemático en aras de conseguir una imputación concreta respetuoso del Principio de Legalidad, ello implica que el agente tenga habilidades informáticas acreditadas, suponer que ya los tiene, incrementaría enormemente la situación de vulnerabilidad de los ciudadanos frente al poder punitivo, de modo que el solo usar las TIC, nos haría delincuentes en potencia.

10. El artículo 11 de la Ley de Delitos Informáticos, le dé mayor reproche penal al agente cuando actúa con el fin de obtener un beneficio económico, esto significa que el objeto del delito, deben ser susceptibles de valoración económica para acreditar el *animus lucrandi*.

11.Concurrencia y participación: Es posible que se presente un concurso aparente con varios delitos, comenzado por los de la misma ley de delitos informáticos como el acceso ilícito, al momento de acceder al sistema para realizar las operaciones,

el atentado contra datos y sistemas informáticos porque en ambos delitos, se actúa de forma similar a la conducta del fraude informático, pero hay intención de obtener provecho ilícito para sí o para otro, también entraría en concurso real los delitos contra el patrimonio, como el hurto. Finalmente, el tipo penal, admite la coautoría, y la participación de cómplices e instigadores.

§ 8. SUPLANTACIÓN DE IDENTIDAD

1. **Genealogía:** El delito aparece el 30 de octubre de 1 998 con la Ley Contra el Robo de Identidad (Identity Theft and Assumption Deterrence Act), y en nuestro país, en la Ley de Delitos Informáticos: Ley 30 096, la Suplantación de Identidad está ubicado en el artículo 9 de la mencionada Ley, la misma que fue modificada por la Ley 30 171, resultando el siguiente texto:

> **Artículo 9. Suplantación de Identidad**
>
> El que, mediante las Tecnologías de la Información o de la Comunicación, suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

2. **Balance histórico:** a) Sobre la naturaleza del delito de suplantación de identidad o fraude de identidad, es un tipo que surge en Estados Unidos, la que comprendió el uso del hardware y software del computador y otros dispositivos como instrumentos de fabricación de documentos de identidad; b) El contenido del injusto del hecho típico, mantiene una pena de menor gravedad; c) Requisitos típicos más notorios, que la suplantación de identidad se realice mediante las TIC.

3. **Tipo objetivo. Los sujetos:** El *sujeto activo*, es cualquier persona natural, y el *pasivo* es cualquier persona natural o jurídica, verbigracia, según WikiLeaks la CIA uso el malware "Hive", para suplantar a la empresa rusa Kaspersky Lab, mientras espiaba, extraía información y controlaba información de los dispositivos de los usuarios, según RT, esta información es importante porque la referida empresa de ciberseguridad fue acusada de cooperar con el Gobierno ruso y maniobrar las Elecciones Presidenciales de Estados Unidos (RT, 2 017, November 9).

4. El artículo 11 de la Ley de Delitos Informáticos, le dé mayor reproche penal al agente cuando es integrante de una organización criminal, abusa de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

5. Tipo objetivo sistemático. La exteriorización de la acción:*Las Tecnologías de la Información y la Comunicación (TIC),* son dispositivos. tecnológicos (hardware y software) que permiten editar, producir, almacenar, intercambiar y transmitir datos entre diferentes sistemas de información que cuentan con protocolos comunes (Cobo Romaní, J., 2 009, p. 312), que importa el medio típico por el cual el agente suplanta la identidad de una persona natural o jurídica, que consiste en ocupar el lugar del otro para perjudicar material o moralmente al sujeto pasivo, verbigracia, publicar o crear un perfil de Facebook de otra persona, y publicar en su nombre con la intención de desprestigiarlo.

6. La conducta de interceptar los datos, es de resultado (Villavicencio Terreros, F., 2 015, p. 19), por tanto, se consuma cuando conforme al plan criminal, se ocasiona el perjuicio material o moral al sujeto pasivo.

7. **Tipo objetivo conglobante. Bien jurídico**: De la redacción del tipo penal se infiere que el bien jurídico corresponde a la *Fe Pública*, que es la confianza colectiva de la comunidad en determinados signos, uniformes, insignias, documentos que pueden probar hechos (Bernate Ochoa, F., 2 010, p. 39; Frisancho Aparicio, M., 2 011, p. 78), su importancia radica en cautelar la seguridad jurídica de la que estánpremunidas las relaciones jurídicas, la que en este Siglo se van creando, modificando y extinguiendo en medio de las TIC.

8. **Tipo subjetivo:** El *dolo*, es la voluntad realizadora del tipo guiada por el conocimiento de los elementos del tipo objetivo sistemático (Zaffaroni, E. R., 2 009a, p. 108), es menester redundar en la necesidad de contar con un perito informático que coadyuve en la tarea de establecer tanto los aspectos objetivos y subjetivos del tipo, el agente debe conocer y querer usar las Tecnologías de la Información y Comunicación, dado que éstos requieren de una habilidad variable, puesto que no todas las TIC son de uso sofisticado, y no se necesita mucho esfuerzo para ingresar datos que correspondan a otra persona, por eso es importante el Informe Pericial.

9.Concurrencia y participación: Es posible que se presente un concurso aparente con varios delitos contra la fe pública, empero se debe considerar el requisito típico más importante que es el uso de las TIC, lo que termina por diferenciarlo. Finalmente, el tipo penal, admite la coautoría, y la participación de cómplices e instigadores.

§ 9. ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS

1. **Genealogía:** El abuso informático, al igual que otros delitos informáticos que se examinaron parágrafos arriba, proviene de la Ley "Counterfeit Access Device and Computer Fraud and Abuse Act", promulgado el 12 de octubre de 1 984, por el Congreso de los Estados Unidos, en ella se prohibió el acceso o todo tipo de forma de divulgación de información para cautelar la seguridad nacional y el secreto empresarial, el fraude y el abuso informático.

2. En nuestro país, en la ley de Delitos Informáticos 30 096, el abuso de mecanismos y dispositivos informáticos está ubicado en el artículo 10 de la mencionada Ley, y éste fue compatibilizado con los criterios del Convenio de Budapest "Convenio sobre la Ciberdelincuencia", con la Ley 30 171 que modificó la Ley 30 096, y tomó base el siguiente texto del Convenio:

> Artículo 6. Abuso de los dispositivos
>
> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:
>
> a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5; ii) Una contraseña, un Código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con

el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y

b) La posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualesquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.

Con la modificatoria de la Ley 30 171, publicada el 10 marzo de 2 014, actualmente el texto del artículo 10 dice:

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, Códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta

servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

2. **Balance histórico:** a) Sobre la naturaleza del delito de abuso de mecanismos y dispositivos informáticos, es un tipo que surge en Estados Unidos la que comprendió la fabricación de hardware y software para la comisión de delitos informáticos; b) El contenido del injusto del hecho típico, mantiene una pena de menor gravedad, pero hay una tendencia a elevarse; c) Requisitos típicos más notorios, que el agente tenga la finalidad de diseñar para la comisión de Delitos Informáticos, a tercero.

3. **Tipo objetivo. Los sujetos:** El *sujeto activo*, es cualquier persona natural, y el *pasivo* es cualquier persona natural o jurídica, verbigracia, desarrollar un generador de series de activación para un programa de uso comercial, vender dispositivos que clonan tarjetas de uso bancario, etc.

4. El artículo 11 de la Ley de Delitos Informáticos, le dé mayor reproche penal al agente cuando es integrante de una organización criminal, abusa de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

5. Tipo objetivo sistemático. La exteriorización de la acción: El tipo prohíbe que de manera intencionada o deliberada e indebida o contra el Ordenamiento Jurídico: Fabricar (producir en serie), diseñar (elaborar un proyecto), desarrollar (realizar), vender (ofrecer), facilitar (proporcionar), distribuir (entregar), importar (introducir en el país) u obtiene para su utilización, uno o más mecanismos (proceso, estructura, máquinas), programas informáticos (conjunto de algoritmos u órdenes, parte lógica),

dispositivos (equipo, aparato), contraseñas (seña secreta para acceder), códigos de acceso (caracteres, números, etc.) o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la Ley de Delitos Informáticos realizados por un tercero, también la acción de ofrecer (comprometerse a dar) o prestar servicio que contribuya a ese propósito, pero siempre a otra persona, no a sí mismo. El delito es de mera actividad (Villavicencio Terreros, F., 2 015, p. 21), por tanto, se consuma cuando conforme al plan criminal, sin importar resultado posterior.

6. **Tipo objetivo conglobante. Bien jurídico**: Con el abuso de mecanismo y dispositivos informáticos, se afecta la disponibilidad e integridad de datos y sistemas informáticos, que es el bien jurídico que debe ser ofendido, ello se desprende del Título 1. del Capítulo II del Convenio sobre la ciberdelincuencia: "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"; dado que el Derecho Penal es sancionador y no constitutivo de bienes jurídicos (Zaffaroni, E. R., 2 016), este bien jurídico, se funda en el derecho fundamental a la confidencialidad e integridad de sistemas informáticos, desarrollado por el Tribunal Constitucional Federal Alemán en los casos BvR 370/07 - 1 BvR 595/07, como una especie de derivación del derecho fundamental a la personalidad (Persönlichkeitsrecht) (Manssen, G., 2 014, June, p. 39), ubicado en el artículo 22 de la Declaración Universal de Derechos Humanos, el inciso 1 del artículo 2 de la Constitución peruana, por la importancia de las computadoras. Internet, teléfonos móviles y las tecnologías para el desarrollo de la personalidad, puesto que el desarrollo reciente de la tecnología de la información ha hecho que los sistemas de tecnología de la información se vuelvan omnipresentes, y su uso es vital para las vidas de muchos ciudadanos.

7. **Tipo subjetivo:** El *dolo*, es la voluntad realizadora del tipo guiada por el conocimiento de los elementos del tipo objetivo sistemático (Zaffaroni, E. R., 2 009a, p. 108), es menester redundar en la necesidad de contar con un perito informático que coadyuve en la tarea de establecer tanto los aspectos objetivos y subjetivos del tipo, el agente debe conocer y querer abusar de los mecanismos y dispositivos informáticos, facilitando, vendiendo, diseñando, desarrollando, etc., con el fin de facilitar la comisión de Delitos Informáticos, este núcleo duro del tipo subjetivo, es sumamente importante, porque la fabricación de dispositivos informáticos que facilitan el uso de la TIC es una práctica común y que es comercializado, y éstos no tienen pese un fin delictivo, el poder punitivo no puede suponer que todo dispositivo o mecanismo siempre es una herramienta para el delincuente, legitimar ello, nos podría a todos en una situación concreta de vulnerabilidad, sería como acusar al que fabrica cuchillos so pretexto de evitar más homicidios, sabemos que hay una finalidad distinta, un carnicero puede usar el cuchillo y no siempre un homicida, en esa lógica, todo desarrollo informático, solo persigue hacer máscómoda la experiencia de vida digital de cada ciudadano, depende del usuario final, que uso lícito o delictivo les pueda dar estos productos.

8.Concurrencia y participación: Es posible que se presente un concurso aparente con varios Delitos Informáticos, puesto que el delincuente informático también fabrica sus propios mecanismos o dispositivos informáticos, empero se debe considerar el requisito típico más importante que es la finalidad de facilitar la comisión de Delitos Informáticos, a terceros, lo que termina por diferenciarlo. Finalmente, el tipo penal, admite la coautoría, y la participación de cómplices e instigadores.

4.6. DIMENSIÓN ESPACIAL Y TEMPORAL DE LOS DELITOS INFORMÁTICOS

§ 1. APLICACIÓN ESPACIAL DE LA LEY PENAL

1. Los Delitos Informáticos son transnacionales, cuando la acción se ejecuta en un país y el resultado en otro país, y más cuando la transferencia de datos se da en redes informáticas internacionales, esto conduce a la desaparición de las categorías clásicas de espacio y tiempo, y con ello a un prototipo de criminalidad transnacional, que se caracteriza por una elevada ubicuidad, grandes riesgos y especial complejidad. (Reyna Alfaro, L. M., 2 002, p. 281; Acurio del Pino, S., 2 007, p. 56, Sieber, U., 2 008, p. 156).

2. Es toda necesidad que el Perú y los países de Latinoamérica suscriban un instrumento internacional de cooperación y persecución de la ciberdelincuencia, pues los clásicos Principios de territorialidad, y extradición, no bastan, por ello la Oficina de las Naciones Unidas contra la Droga y el Delito, resalta la cuestión de qué país puede reclamar apropiadamente jurisdicción penal sobre delitos cibernéticos, teniendo en cuenta que algunas veces la *locus commissi delicti* no es fácilmente discernible, debido a que el ciberespacio no puede describirse en términos de territorio (2 012, p. 124).

3. A modo de ejemplo, un hacker peruano que reside en China en coautoría con hacker coreanos ubicados en Irán, deciden atentar contra los datos informáticos de los servidores de correo electrónico del Gobierno de la India, para evitar ser rastreados e identificados, usan varios servidores de proxy de países europeos, y usan servicios de comunicación ofrecidos en la Darknet, ¿Qué legislación le es aplicable a los agentes?, ¿Qué podemos hacer si en la India no está previsto los Delitos Informáticos, ¿Qué

mecanismos de cooperación existen si en todos los países involucrados no han suscrito tratados?, si bien estas interrogantes pueden resolverse con el Derecho Penal Internacional, es una tarea compleja para el Perito Informático, señalar el lugar de acción y del resultado, o los efectos, sin mecanismo de cooperación, será un gran desafío a los sistemas de justicia de cada país, evitar la impunidad. Esperemos que pronto el Perú se adhiera al Convenio sobre cibercriminalidad (Convenio de Budapest), en cumplimiento con la Octava Disposición Complementaria y Final de la Ley de Delitos Informáticos, sobre el imperativo de promover la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los Delitos Informáticos.

4. El Código Penal peruano de 1991, para la aplicación espacial nos ofrece, los siguientes Principios: a) Principio de Territorialidad (Artículo 1), que estipula que la Ley Penal peruana se aplica a todo el que comete un hecho punible en el territorio de la República, salvo las excepciones contenidas en el Derecho Internacional, b) Principio de Extraterritorialidad (Artículo 2), c) Principio real o de defensa (Artículo 2), d) Principio de personalidad activa y pasiva (Artículo 2), e) Principio de representación (Artículo 3), por el último f)Principio de ubicuidad (Artículo 5), que establece que el lugar de comisión de un delito es aquél en el cual el autor o partícipe ha actuado u omitido la obligación de actuar o en el que se producen sus efectos, de todos modos el problema radicará cuando el delito se originó en otro país, y son varias las naciones comprometidas en el hecho delictivo.

§ 2. APLICACIÓN TEMPORAL DE LA LEY PENAL

1. En cuanto el aspecto temporal de la comisión de los Delitos Informáticos, no pasa de lo ordinario, si el delito se dio en nuestro país, se debe emplear los Principios de aplicación temporal del Código Penal: a) Principio de combinación (artículo 6), que señala que la ley penal aplicable es la vigente en el momento de la comisión del hecho punible. No obstante, se aplicará la más favorable al reo, en caso de conflicto en el tiempo de leyes penales. Si durante la ejecución de la sanción se dictare una ley más favorable al condenado, el Juez sustituirá la sanción impuesta por la que corresponda, conforme a la nueva ley; b) Retroactividad benigna (artículo 7), afirma que si, según la nueva ley, el hecho sancionado en una norma anterior deja de ser punible, la pena impuesta y sus efectos se extinguen de pleno derecho; c) Leyes temporales (artículo 8), prescribe que las leyes destinadas a regir sólo durante un tiempo determinado se aplican a todos los hechos cometidos durante su vigencia, aunque ya no estuvieren en vigor, salvo disposición en contrario, por último, d) Momento de comisión del delito (artículo 9), que sostiene que el momento de la comisión de un delito es aquél en el cual el autor o partícipe ha actuado u omitido la obligación de actuar, independientemente del momento en que el resultado se produzca.

2. Siguiendo el ejemplo plateando en el apartado anterior, el ataque a los datos informáticos, se torna complejo, si hay conflicto de sucesión de leyes en el tiempo para cada país, lo que puede suceder si entre la acción y el resultado hay mucho tiempo, días, semanas, meses, como fraudes informáticos en bancos, que suelen prologarse durante el tiempo; en todo caso, la solución ha de ser creativa, empleando cada uno de los Principios del Código Penal, y de contar con Cooperación Internacional, éstos deben

premunirse de protocolos de aplicación de leyes, esto importa uniformizar criterios en sede fiscal y judicial.

4.7. CONSIDERACIONES DE POLÍTICA CRIMINAL SOBRE LOS DELITOS INFORMÁTICOS

§ 1. POLÍTICA CRIMINAL Y LOS DELITOS INFORMÁTICOS

1. Para este apartado, es menester reflexionar a partir de la Criminología Cautelar, puesto que cuando el Derecho Penal está políticamente ciego –como afirma el maestro Raúl Zaffaroni– es un "mono con navaja" (2 011, p. 18), es cierto que la criminalización mediática, tiende a considerar todo conflicto social como delito, para decir que se "hace algo", de modo que se potencia más el poder punitivo, y con ella se legitima más la sociedad de control, denominándola Sociedad de la Información o Sociedad del Riesgo, donde el poder de vigilancia del poder punitivo con los Delitos Informáticos se proyecta a la vida digital de las personas, en otras palabras todas las agencias ejecutivas (policías, fiscales, servicio de inteligencia, etc.) tienen la posibilidad de vigilar lo que sucede en el mundo digital, que es en gran medida nuestra propia vida la que se ve expuesta ante los ojos y manos de quienes están en el centro del mundo, quienes gobiernan la sociedad de control, gracias a toda la minera de datos que recopilan y tratan las agencias ejecutivas, las mismas que son compartidas con las empresas, siendo también éstas las que comparten información a servicios de inteligencia, de todos modos, ser usuario o desarrollador de las TIC, no hace potenciales delincuentes de manera que se habilita el poder de vigilancia de las agencias ejecutivas para que en un momento dado se incremente nuestra vulnerabilidad hasta una situación concreta en la que el semáforo dará luz verde al poder punitivo; frente a este problema, el penalista no tiene otra opción que someterse al Principio de Legalidad, legitimar lo ya

prescrito por lo de arriba, de igual modo, la periferia seguir al centro del mundo, pero, el Derecho Penal – saber jurídico que proyecta decisiones– y la Criminología otro saber que, hace hablar a los muertos, deben deslegitimar al poder punitivo en la sociedad de control que vivimos.

2. Los actos de poder, traducidos en la criminalización de los conflictos sobre la ciberdelicuencia, permitiendo extenderse más al poder punitivo, cuyos efectos de su ejercicio selectivo son que todas las personas que usamos las Tecnologías de la Información y Comunicación que importa el manejo de datos y sistemas informáticos, seamos sospechosos o potenciales agentes de Delitos Informáticos, por ende, hay mayor vulnerabilidad de las personas que manejan teléfonos móviles inteligentes (Smartphone), ordenadores portátiles (laptop), tabletas digitales (Tablet), etcétera, con la vigilancia ejercida por los agentes ejecutivos, hay reducción de privacidad y libertad, con ello mantiene en funcionamiento la sociedad de control, al semejante a la trama de la película “The Truman Show”, en la que toda la vida pública y privada de Truman Burbank era observado por televidentes de un programa de televisión.

3. El 30 de diciembre de 2 016 se publicó un estudio en el Diario El País, elaborado por el Instituto para la Integración de América Latina (INTAL), que revela que más de la mitad de los latinoamericanos que apenas tienen acceso a los bienes básicos, están sin embargo conectados en las redes sociales (Marcial Perez, D.), y la Unión Internacional para las Telecomunicaciones (UIT) ha determinado que casi uno de cada cuatro usuarios de Internet en el mundo se encuentran entre la franja de los 15 a los 24 años de edad (EFE, 2 017, July 31), por eso sostenemos que los jóvenes serían los más expuestos de la criminalización, y los adultos mayores, los menos vulnerables,

empero, que los jóvenes de hoy puedan usar redes sociales, no es suficiente para concluir que tenga acceso pleno al Internet, y por tanto tengan todas las posibilidades de actuar como un hacker, sabemos que el Internet que los ISP (proveedores de servicio de Internet) ofertan en Latinoamérica, no son los mejores en la periferia (Gestión, 2 016, December 19), y que la infraestructura de redes, tampoco es la mejor (BBC Mundo, 2 016, January 4), en fin, solo un verdadero hacker podría lidiar con la adversidad tecnológica de nuestros países, no todos los jóvenes son comunes y silvestres, salvo que se use solo ingeniería social que no requiere conocimientos de informática, también se dice que la existencia de los Delitos Informáticos ya no está confinada a las capas desheredadas de la población; sino por el contrario, ésta se extiende a las capas superiores y medias (Heredia Obregón, S., 2 015), afirmación que no deja de tener razón si nos referimos a los Gobiernos como sujetos activos por autoría mediata de delitos informáticos, sin embargo en la sociedad de control, no hay WhiteCollar, todos somos potenciales sujetos activos, por eso nos vigilan, en especial a los jóvenes en tanto se mantengan como usuarios mayoritarios y frecuentes.

4. Considerando lo anterior, los efectos nocivos de la selectividad serían alimentar un estereotipo de hacker en lo jóvenes de generación digital, el nuevo chivo expiatorio, para abrir camino al Estado de Policía, y no hay beneficio en ello, puro efecto simbólico como una aparente seguridad y confianza en los habitantes que no serán víctimas de fraude informático, acceso ilícito, etc., frente a este problema, solo nos queda deslegitimar al poder punitivo en la sociedad de control con el derecho penal humano, o digamos el Derecho Penal informático humano, ésta sería una forma jurídica de limitar la selectividad y los efectos nocivos del poder punitivo.

5. Los Delitos Informáticos como panóptico del poder punitivo, otorga un poder de vigilancia los servicios secretos de los Estados, y en nombre de perseguir a los ciberdelicuentes, alimentando una metamorfosis a un Estado totalitario, controlando cada movimiento de Internet, con ello se mantendrá la sociedad de control; el poder mediático por su parte alimenta el estereotipo de hacker, el poder financiero es tributario de la sociedad de control, pues éste con todo el poder de controlar la información, puede continuar asegurando su participación en la política, y en un Estado totalitario puede ser parte del Deep State término acuñado por Mike Lofgren (2 016), que decide hasta dónde llegará la soberanía de un Estado.

6. En un Estado poco democrático y con el poder jurídico debilitado, los tipos de Delitos Informáticos pueden servir para injerencias en la privacidad de personas y atentar contra los derechos humanos, puesto en la sociedad de control, necesita de vías legítimas de extender su poder de vigilancia, como los tipos tienen doble cara como una moneda, una para reducir y otra para habilitar el poder punitivo, en la criminalización secundaria, cuando la selectividad del poder punitivo no es contenido, éste reduce ostensiblemente la privacidad de las personas, porque la interceptación, el acceso a sistemas, la interferencia de datos y sistemas, el uso de agentes encubiertos, está legitimado porque las agencias de inteligencia buscan conseguir seguridad digital a un costo alto de invasión de la privacidad de cada ciudadano, por investigar a uno, la cadena de datos, se masifica a su familia, a los amigos de la familia, a sus amigos, a los amigos de los amigos, a los compañeros de trabajo, y a sus respectivas familias así sucesivamente, como lo señaló Edward Snowden, sus afirmaciones se vienen confirmando con WekiLeaks, que ha revelado, que CIA, NSA, en el caso de Estados Unidos, pueden vigilarnos con las Webcam, las cámaras de los Smartphone y Tablet,

recopilar información de los Smarttv, electrodomésticos con Internet, leyendo nuestro mensaje de correo electrónico, cuentas bancarias y acceder a otras informaciones, el discurso legitimante, dirá que se trata de actividades para evitar el ciberterrorismo, o defendernos del ataque de otro país, en fin nos veremos obligados a desconectarnos del Internet. Además en un Estado de Policía, nada impide pensar que se pueda vender la información o comercializarse con fines espurios, dice el dicho "información es poder", y las empresas, Partidos Políticos, organizaciones criminales, puede sacar provecho de información personal almacenada en bases de datos sistematizadas de los servicios secretos de inteligencia de cada país, verbigracia venta de correos electrónicos, registros personales, información militar; comunicaciones por redes sociales y servicios de mensajería, todo obtenido y comerciado por el Gobierno y empresas de hegemonía económica, quisiéramos pensar que la información vendida solo serviría para descubrir amantes, el llamado "Loveint" (Gabbatt, A., 2 013, August 24), por desgracia, el tráfico de información militar podría aumentar las posibilidades de desencadenar otra guerra mundial, genocidios, persecución a cualquier persona y tendríamos más muertos y daños a nuestra casa común. De otro lado, no podemos ser ingenuos, las agencias ejecutivas son vulnerables a la corrupción, por ello no descartamos la posibilidad que se presten a la manipulación de la información recopilada, conformar grupos de espionaje privado, a vender información confidencial, extorsión, acoso sexual, etcétera.

7. En cuanto a si los Delitos Informáticos ayudarían a prevenir el crimen organizado, el terrorismo, y otros delitos complejos y transnacionales, creemos que sí, de algún modo, con mayor resultado en los Países del Centro, por lo menos con la ayuda del poder mediático hasta cierto punto, pero como el poder punitivo es corruptible y el aparato político quiere el mayor control, no es agradable exponerse al

riesgo de un golpe de Estado, por eso con el tiempo la prevención será más intensa, se recurrirá a tipificar las tentativas, los delitos culposos, a emplear más tipos en blanco, a incrementar las penas adoptando una Política Criminal según una criminología mediática para reforzar y legitimar un Estado Autoritario con ropaje democrático, el discurso de la lucha contra el terrorismo, las drogas, ahora el crimen organizado mediante las TIC, es eficaz para domesticar a los países periféricos, empero, esta prevención y persecución, se degrada a medida que nos alejamos del Centro, como sabemos la policía también es conformada por la selectividad del poder punitivo, y la tecnología con la cuenta no es equiparable a la del centro, por ello el control de los espacios virtuales se realiza con tecnología rudimentaria, es lo más lógico, puesto que la inversión en tecnología no es la misma que los países del centro que están forjando la "Industria 4.0" (DW, 2 017, June 7); mientras que los países periféricos, no se dan las condiciones para convivir con robots y fábricas inteligentes.

§ 2. PREVENCIÓN DE LOS DELITOS INFORMÁTICOS

1. La tarea de prevenir la comisión de Delitos Informáticos, también es al mismo tiempo, la de prevenir la vigilancia del poder punitivo en la sociedad de control, pues estos fenómenos estarán siempre entrelazadas, ya lo mencionamos en otro apartado, que los Delitos Informáticos habilitan poder punitivo, y a la vez nos ofrece las pautas para su reducción, es una moneda de dos caras; en este sentido, se debe prevenir la comisión de ciber ataques y reducir el poder de vigilancia del poder punitivo.

2. Para prevenir la comisión de Delitos Informáticos, seguiremos la "Mini guía de seguridad informática " de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), de la que extraemos las siguientes recomendaciones: a) Tener

cuidado con la información que se publica en Internet, eso implica configurar la privacidad de nuestras cuentas virtuales para que solo amigos y familiares puedan ver lo que publicamos, b) No compartir videos e imágenescomprometedoras por chat o redes sociales, c) No usar la webcam con desconocidos, d) No responder mensajes que solicitan información personal, como cuentas de usuario, contraseñas y otros datos, e) No hacer clic en enlaces ni descargar archivos adjuntos de mensajes sospechosos (spam, remitentes desconocidos), f) Pensar antes de compartir contenidos en Internet (no compartir fotos de hijos menores), d) No aceptar invitaciones de Internet de personas extrañas o en las que no confiamos, e) No descargar programas y archivos que no conocemos y de sitios desconfiables, f) No usar una contraseña para todas las cuentas, hay que cambiarla periódicamente, g) Habilitar mecanismos de seguridad de los dispositivos, y borrar información personal si vendemos los equipos, h) Aprender y enseñar a los demás cómo prevenir la comisión de Delitos Informáticos. En este punto nos parece conveniente exigir el cumplimiento de la Ley 30 254 "Ley de promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por niños, niñas y adolescentes".

3. Respecto a la vigilancia masiva, nos parece conveniente difundir y observar los "Principios Internacionales de Derechos Humanos sobre Vigilancia de las Comunicaciones", escrito colaborativamente por la Electronic Frontier Foundation y otras organizaciones de privacidad y activistas, considerando que la *intimidad,* es un derecho humano fundamental y es cardinal para el mantenimiento de sociedades democráticas, estos son: (1) *Legalidad* (cualquier limitación a los derechos humanos debe ser prescrita por ley), (2) *Objetivo Legítimo* (las leyes sólo deberían permitir la Vigilancia de las Comunicaciones por parte de autoridades estatales específicas para

alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática), (3) *Necesidad* (leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo, (4) *Idoneidad* (cualquier caso de vigilancia de las comunicaciones autorizado mediante Ley debe ser apropiado para cumplir el objetivo legítimo específico identificado), (5) *Proporcionalidad* (la vigilancia de las comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática), (6) *Autoridad judicial competente* (las decisiones relacionadas con la vigilancia de las comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente, (7) *Debido Proceso* (el Debido Proceso exige que los Estados respeten y garanticen los derechos humanos de las personas asegurando que los procedimientos legales que rigen cualquier interferencia con los derechos humanos estén enumerados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público en general), (8) *Notificación del usuario* (aquellos cuyas comunicaciones están siendo vigiladas deben ser notificados de la decisión de autorizar la Vigilancia de Comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización), (9) *Transparencia* (los Estados deben ser transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, reglamentos, actividades, poderes o autoridades), (10) *Supervisión Pública* (los Estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones), (11) *Integridad de las comunicaciones y sistemas* (los Estados no deben obligar a los proveedores de servicios

o proveedores de “hardware” o “software” a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado), (12) *Garantías para la cooperación internacional* (cuando la legislación de más de un Estado pueda aplicarse a la vigilancia de las comunicaciones, se adopte el estándar disponible con el mayor nivel de protección para las personas) y (13) *Garantías contra el acceso ilegítimo y derecho a recurso efectivo* (los Estados deben promulgar leyes que penalicen la vigilancia de las comunicaciones ilegal por parte de actores públicos o privados). Finalmente debemos seguir la recomendación de Richard Stallman (2 013), de usar Software Libre, no compartir datos personales de amigos a otros, dejar dispersos nuestros archivos, impedir su acceso, pagar en efectivo, evitar identificarse en los sitios web, pedir que los policías usen cámaras de video todo el tiempo, que la investigación a delincuentes sea por delitos específicos y con orden judicial, usar servicios de correo electrónico que países que no cooperarían con el Gobierno de los EE.UU., pedir que los ISP y compañías de teléfono conserven por mucho tiempo los registros de usos o actividad de sus usuarios, abolir la lista de prohibición de vuelos a los EE.UU., pedir que los pagos de telepeaje sean anónimos, usar sistema de pago anónimo y solicitar el rediseño de sistemas para que no recolecten datos de los usuarios.

V. CONCLUSIONES

GENERAL

El Derecho Penal Informático (humano), es el saber jurídico penal que, mediante la interpretación de leyes penales sobre Delitos Informáticos, propone a los agentes jurídicos un sistema reductor del poder de vigilancia del poder punitivo en la sociedad de control, e impulsar el poder jurídico con el fin de preservar los espacios de libertad y privacidad de las personas.

ESPECÍFICOS

Los límites u horizonte de proyección del Derecho Penal Informático, se explica por su propia definición como saber jurídico que interpreta Delitos Informáticos con el método dogmático deslegitmante del Derecho Penal Humano del maestro Raúl Zaffaroni, para reducir los efectos del poder de vigilancia del poder punitivo en la sociedad de control, resultando el "Derecho Penal Informático Humano", que tiene por objeto estudio a la seguridad jurídica, y las leyes penales sobre Delitos Informáticos como objeto de interpretación; tiene la función de reducir el poder de vigilancia del poder punitivo; se caracteriza por ser público, represivo, continuo, fragmentador y normativo.

La interdisciplinariedad del Derecho Informático y el Derecho Penal, se explica por su correspondencia de saberes jurídicos, que es de forma secante por la superposición en sus horizontes de proyección para la adecuada interpretación de los Delitos Informáticos, la sinergia de ambos, garantizar el nullum crimen sine conducta mediante una unidad funcional de trabajo de contención al poder punitivo, el Derecho

Penal aporta sus Principios constructivos y su dogmática deslegitimante, y del Derecho Informático se ocupa de la comprensión de los fenómenos informáticos.

El Derecho Penal Informático, como saber jurídico penal, tiene (a) Fuente de Conocimiento, que son todas las leyes sobre Delitos Informáticos y (b) De Información que se refiere a la bibliografía penal y de otros saberes, y como legislación penal, tiene (a) Fuentes de Conocimiento, que son las leyes penales constitucionales (lícitas) sobre delitos informáticos y (b) De Producción, que se refiere a instituciones u órganos constitucionalmente habilitadas para la sanción de leyes penales, entre ellos los Delitos Informáticos.

El Delito Informático (computer crime / computerkriminalität), es definido de manera (a) Formal, como acción u omisión prohibida por la ley penal sobre delitos informáticos; (b) Material, como conducta final que ofenden bienes jurídicos relacionados a las Tecnologías de la Información y la Comunicación, y (c) Analítica, como conducta, típica, antijurídica y culpable que tiene como medio u objeto de protección a las Tecnologías de la Información y Comunicación.

Los Delitos Informáticos en el Ordenamiento Jurídico peruano, están previstos en la Ley 30 096 “Ley de Delitos Informáticos”, modificado por la Ley 30 171 que se inspiró en el Convenio sobre la Ciberdelincuencia; los tipificados son: (a) Acceso ilícito, (b) Atentado a la integridad de datos informáticos, (c) Atentado a la integridad de sistemas informáticos, (d) Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, (e) Interceptación de datos informáticos, (f) Fraude informático, Suplantación de identidad y Abuso de mecanismos y dispositivos informáticos, los

mismos que se encuentran tipificados en varios países, entre ellos Estados Unidos, Alemania, Francia, España, Chile, Argentina, y Ecuador.

Sobre la Aplicación Espacial de la ley, los Delitos Informáticos son transnacionales, cuando la acción se ejecuta en un país y el resultado en otro país, y cuando la transferencia de datos se da en redes informáticas internacionales. En cuanto el aspecto temporal de la comisión de los delitos informáticos, se deben emplear los Principios de aplicación temporal del Código Penal.

La criminalización mediática, ha fomentado los Delitos Informáticos, y con ella se potencia más el poder punitivo, se legitima más la sociedad de control y su poder de vigilancia, puesto que el poder punitivo se proyecta a la vida digital de las personas, permitiendo que agencias ejecutivas tengan posibilidad de vigilar lo que sucede en el mundo digital, facilitando a quienes están en el centro del mundo, gobernar la sociedad de control; esto tiene efectos nocivos como alimentar un estereotipo de hacker en los jóvenes de generación digital, abrir camino al Estado de Policía, y corrupción con todos los datos recopilados. Para la prevención de los delitos informáticos y del poder de vigilancia, proponemos(a) Tener cuidado con la información que se publica en Internet, (b) No compartir videos e imágenes comprometedoras por chat o redes sociales, (c) No usar la webcam con desconocidos, (d) No responder mensajes que solicitan información personal, como cuentas de usuario, contraseñas y otros datos, (e) No hacer clic en enlaces, ni descargar archivos adjuntos de mensajes sospechosos, (f) Difundir y observar los "Principios Internacionales de Derechos Humanos sobre Vigilancia de las Comunicaciones".

VI. RECOMENDACIONES

El futuro de la Investigación estriba en continuar desarrollando un proyecto de jurisprudencia penal en materia de Delitos Informáticos con la dogmática penal del Derecho Penal Informático humano y la Criminología Cautelar.

Proponer un sistema interpretativo deslegitimante para la Convención sobre Ciberdelincuencia (Convenio de Budapest), conforme al derecho internacional de los derechos humanos.

Formular propuestas legislativas que se inspiren en los "Principios Internacionales de Derechos Humanos sobre Vigilancia de las Comunicaciones" para reducir el poder de vigilancia de las agencias ejecutivas.

Proponer la creación de una Fiscalía Especializada en Tecnologías de la Información y Comunicación (TIC).

VII. REFERENCIAS

Acosta Patroni, A. (2 003). *Hacking, cracking y otras conductas ilícitas cometidas a través de internet*. Universidad de Chile. Retrieved from http://repositorio.uchile.cl/bitstream/handle/2250/114475/de-acosta_a.pdf?sequence=1&isAllowed=y

Acurio Del Pino, S. (2 007). *Delitos Informáticos: Generalidades*. Retrieved from http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Ahmed, Azam. Perlroth, N. (2 017, June 19). "Somos los nuevos enemigos del Estado": el espionaje a activistas y periodistas en México. *The New York Times Company*. New York. Retrieved from https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

Alcántara, J. F. (2 008). *La sociedad de control Privacidad, propiedad intelectual y el futuro de la libertad*. Barcelon, España. Retrieved from https://www.versvs.net/wp-content/libros/la-sociedad-de-control/jose-alcantara-la-sociedad-de-control.pdf

AllClear ID. (2 012). Online Impersonation vs. Identity Theft: Is There a Difference? Retrieved from https://www.allclearid.com/personal/2012/12/online-impersonatin-vs-identity-theft/

Amnistía Internacional. (2 014). Nueva herramienta para que víctimas de espionaje puedan detectar la actividad de vigilancia del gobierno. Retrieved June 5, 2017, from https://www.es.amnesty.org/footer/conocenos/test/noticias/noticia/articulo/nueva-herramienta-para-que-victimas-de-espionaje-puedan-detectar-la-actividad-de-vigilancia-del-gob/?L=0&cHash=f399bc25c3f386576719b057eead2dbc

Arata Salinas, A. A. (2 002). *Las nuevas tecnologías de información y problemática jurídica del comercio electrónico*. Universidad Nacional Mayor de San Marcos. Retrievedfromhttp://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Human/Arata_S_A/T_completo.pdf

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS. (1948, December 10). DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS. Retrieved from http://www.un.org/es/documents/udhr/index_print.shtml

Ashiq, J. A. (2 005). Insider vs. Outsider Threats: Identify and Prevent. Retrieved from http://resources.infosecinstitute.com/insider-vs-outsider-threats-identify-and-prevent/

Asociación para el Progreso de las Comunicaciones. (2 010). Carta de los derechos en Internet de APC. In *Efectos de las TICs sobre los Derechos Humanos* (1st ed., pp. 57–63). Barcelona: Institut de Drets Humans de Catalunya (IDHC). Retrieved from https://www.guao.org/sites/default/files/biblioteca/Efectos de las TICs sobre los Derechos Humanos.pdf

Barreda Tamayo, O. (1 997). *Selección de textos de Mario Bunge*. Arequipa: UNSA.

BBC Mundo. (2016, January 4). Los países del mundo con la mejor y peor infraestructura. *BBC*. Retrieved from http://www.bbc.com/mundo/noticias/2016/01/160104_economia_paises_mejor_infraestructura_lf

BBC Mundo. (2 017, June 27). Un nuevo ciberataque de gran escala afecta a compañías e instituciones de todo el mundo. Retrieved from http://www.bbc.com/mundo/noticias-internacional-40422053

Beccaria, C. (1 993). *Tratado de los delitos y de las penas*. Buenos Aires, Argentina: Heliasta. Retrieved from

https://criminologiacomunicacionymedios.files.wordpress.com/2013/08/beccaria-cesar-tratado-de-los-delitos-y-de-las-penas.pdf

Beck, U. (1 998). *La sociedad del riesgo: hacia una nueva modernidad*. Barcelona, España: Paidós.

Beck, U. (2 000). *Un nuevo mundo feliz: la precariedad del trabajo en la era de la globalización*. Barcelona, España: Paidós.

Beling, E. von. (2 002). *LA DOCTRINA DEL DELITO-TIPO*. Buenos Aires, Argentina: Librería El Foro.

Benedicto XVI, P. (2 009). *Caritas in veritate : sobre el desarrollo humano integral en la caridad y en la verdad* (1st ed.). Lima, Peru: Paulinas. Retrieved from http://w2.vatican.va/content/benedict-xvi/es/encyclicals/documents/hf_ben-xvi_enc_20090629_caritas-in-veritate.pdf

Bernal Torres, C. A. (2 010). *Metodología de la investigación : administración, economía, humanidades y ciencias sociales* (3a ed.). México: Prentice-Hall/Pearson Educación. Retrieved from http://eva.sepyc.gob.mx:8383/greenstone3/sites/localsite/collect/ciencia1/index/assoc/HASHe5b1.dir/11050004.pdf

Bernate Ochoa, F. (2 010). *Los delitos contra la fe pública*. Bogotá, Colombia: Editorial Universidad del Rosario. Retrieved from https://books.google.com.pe/books?id=rnl4cRO-z6kC

Blossiers Mazzini, Juan José; Calderón García, S. B. (n.d.). DELITOS INFORMATICOS: CAMINO A LA IMPUNIDAD. Retrieved from http://www.alfa-redi.org/sites/default/files/articles/files/blossiers.pdf

BOSWORTH, S., KABAY, M. E., & WHYNE, E. (2 014). *Computer Security Handbook* (6th ed.). New Jersey, United States of America.

Bramont Arias Torres, L. M. (2 008). *Manual de derecho penal:parte general*. Lima, Perú: Eddili.

Bramont-Arias Torres, L. A. (2 000). Delitos Informáticos. *Revista Peruana de Derecho de La Empresa*, *51*. Retrieved from http://webcache.googleusercontent.com/search?q=cache:aPTvXmOGIxkJ:www.asesor.com.pe/teleley/5Bramont-51.pdf

Bundesverfassungsgericht. (2 008, February 27). BvR 370/07 - BvR 595/07. Retrieved from http://www.bverfg.de/e/rs20080227_1bvr037007.html

Burkett, R. (2 013). An Alternative Framework for Agent Recruitment: From MICE to RASCLS. *Studies in Intelligence*, *57*. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE to RASCALS.pdf

Campoli, G. A. (2 013). *Delitos informáticos en la legislación mexicana*. México. Retrieved from https://www.scribd.com/doc/232525963/Campoli-Gabriel-Andres-Delitos-Informaticos-en-La-Legilacion-Mexicana

Castellanos Hernández, E. (2 006). *Temas de Dererecho Informático* (1st ed.). México: Secretaría de Gobernación de México. Retrieved from http://www.ordenjuridico.gob.mx/Publicaciones/Libros2006/Derecho Informatico.pdf

Catoira, F. (2 012). Consejos para evitar un ataque de denegación de servicio. Retrieved from https://www.welivesecurity.com/la-es/2012/03/28/consejos-ataque-denegacion-servicio/

Chiara Galván, E. R. (n.d.). *Manual de informática jurídica*. Lima, Perú: Universidad Inca Garcilaso.

Chomsky, N. (1 998). *La cultura del terrorismo*. Barcelona, España: Editorial Popular.

Cobo Romaní, J. C. (2009). El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento. *Zer*, *14*(27), 295–318. Retrieved from http://www.ehu.eus/zer/hemeroteca/pdfs/zer27-14-cobo.pdf

Collin, B. C. (n.d.). The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. Retrieved from http://www.crime-research.org/library/Cyberter.htm

ComScore. (2 016). *Futuro Digital Global 2016 - comScore, Inc*. Retrieved from https://www.comscore.com/lat/layout/set/popup/content/download/36941/2097615/version/3/file/2016-Global-Digital-Future-In-Focus-Report.pdf

ComScore. (2 015). *Futuro Digital América Latina 2015 – comScore*. Retrieved from https://es.slideshare.net/delgadocristian/2015-latam-digitalfutureinfocus

Congreso de la República del Perú. (2003, December 4). Dictamen de la Comisión de la Mujer y Desarrollo Social. Lima. Retrieved from http://www2.congreso.gob.pe/Sicr/TraDocEstProc/TraDoc_condoc_2001.nsf/d99575da99ebfbe305256f2e006d1cf0/048d71e53d235083052574be00588b9a/$FILE/01407DCMAY041203.pdf

Congreso de la República del Perú. (2 014, March 10). LEY QUE MODIFICA LA LEY 30096, LEY DE DELITOS INFORMÁTICOS [Ley 30171]. Retrieved from http://busquedas.elperuano.com.pe/download/url/ley-que-modifica-la-ley-30096-ley-de-delitos-informaticos-ley-n-30171-1059231-2

Congreso de la República del Perú. (2 013, October 23). Fe de Erratas de la Ley 30096. Retrieved from http://busquedas.elperuano.com.pe/download/full/1CmCEqzwa-jBHlBNcWpUXu

Congreso de la República del Perú. (2 013, October 22). Ley de Delitos Informáticos [Ley 30096]. Retrieved from http://busquedas.elperuano.com.pe/download/url/ley-de-delitos-informaticos-ley-n-30096-1003117-1

Congreso de la República del Perú. (2 000, July 17). Ley que incorpora los delitos informáticos al Código Penal [Ley 27309].

CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS. (1 999, May 17). SE REFORMAN DIVERSAS DISPOSICIONES EN MATERIA PENAL. Retrieved from http://www.diputados.gob.mx/LeyesBiblio/ref/cpf/CPF_ref75_17may99.pdf

Congreso Nacional de Chile. (1 993, June 7). TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA [Ley N° 19223]. Retrieved from https://www.leychile.cl/Navegar?idNorma=30590

Congreso Nacional de Ecuador. (2002, April 17). LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS [Ley N°. 2002-67]. Retrieved from http://www.oas.org/juridico/pdfs/mesicic4_ecu_comer.pdf

Corte Suprema de Justicia. Primera Sala Penal Transitoria. (2 009, January 16). R. N. Nº 4403-2008 [MP Neyra Flores]. Retrieved from http://www.nomos.pe/jurisprudencia/R-N-4403-2008.pdf

Council of Europe. (2 001, November 23). Convenio sobre la Ciberdelincuencia [Convenio]. Budapest. Retrieved from http://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Creus, C. (1 992). *Derecho penal: Parte General* (3rd ed.). Buenos Aires, Argentina: Astrea.

Curras Puente, E. (1 988). *La información en sus nuevos aspectos*. (Paraninfo S.A., Ed.) (1st ed.). Madrid, España. Retrieved from http://www.uam.es/personal_pdi/ciencias/ecurras/lainformacionaspectos.pdf

Cyber Crime Investigation Cell. (n.d.). Hacking. Retrieved from http://cybercellmumbai.gov.in/html/cyber-crimes/hacking.html

Del Peso Navarro, E. (2 001). *Peritajes Informáticos* (2nd ed.). Madrid, España: Díaz de Santos, S.A. Retrieved from https://books.google.com.pe/books?id=IUe2bRI8gxUC

DW. (2 017, June 7). Hecho en Alemania - Industria 4.0: tecnología versus tradición. *DW Español*. Retrieved from http://www.dw.com/es/hecho-en-alemania-industria-40-tecnología-versus-tradición/av-39142375

DW. (2 017, October 11). Seúl acusa a Pyonyang de haber robado datos militares. Retrieved from http://www.dw.com/es/seúl-acusa-a-pyonyang-de-haber-robado-datos-militares/a-40908303

DW. (2 017, May 12). Ciberataque mundial pone en riesgo sistemas informáticos de más de 70 países | El Mundo | DW | 12.05.2017. Berlín. Retrieved from http://www.dw.com/es/ciberataque-mundial-pone-en-riesgo-sistemas-informáticos-de-más-de-70-países/a-38824106

DW. (2 017, May 25). La darknet | Todos los contenidos | DW | 27.05.2017. DW. Retrieved from http://www.dw.com/es/la-darknet/av-39003776

DW. (2 017, June 2). Merkel: "Continuemos unidos a favor de nuestra Madre Tierra" | El Mundo | DW | 02.06.2017. Berlín. Retrieved from http://www.dw.com/es/merkel-continuemos-unidos-a-favor-de-nuestra-madre-tierra/a-39092027

Economist, T. (2 008). *El futuro de la tecnología* (1st ed.). Lima, Perú: The Economist.

EFE. (2 017, July 31). El 80 por ciento de los jóvenes en 104 países tienen acceso a internet, según reveló la ONU. *EFE*. Ginebra. Retrieved from https://www.efe.com/efe/america/tecnologia/el-80-por-ciento-de-los-jovenes-en-104-paises-tienen-acceso-a-internet-segun-revelo-la-onu/20000036-3340329

El Mundo. (2 017, July 16). España extraditaría a "hacker" ruso a EE. UU. *DW*. Retrieved from http://www.dw.com/es/españa-extraditaría-a-hacker-ruso-a-ee-uu/a-39710557

Electronic Frontier Foundation y otras organizaciones. (n.d.). *NECESARIOS & PROPORCIONADOS PRINCIPIOS INTERNACIONALES SOBRE LA APLICACIÓN DE LOS DERECHOS HUMANOS A LA VIGILANCIA DE LAS COMUNICACIONES*. Retrieved from https://necessaryandproportionate.org/files/2016/03/04/spanish_principles_2014.pdf

Espinoza Coila, M. (2 015). LA NECESIDAD DE UNA INTERDISCIPLINARIEDAD SECANTE ENTRE EL DERECHO PENAL Y EL DERECHO INFORMÁTICO. Retrieved from http://www.unap.edu.pe/web4/la-necesidad-de-una-interdisciplinariedad-secante-entre-el-derecho-penal-y-el-derecho-informatico

Espinoza Coila, M. (2 014). Los delitos informáticos en el Perú: Panóptico del poder punitivo. *Taripaña*, *6*, 13–16.

Espinoza Coila, M. (2 013). EL PODER Y EL PUEBLO EN EL ESTADO. Retrieved June 3, 2017, from http://www.unap.edu.pe/web4/el-poder-y-el-pueblo-en-el-estado

Ferrajoli, L. (2 004). *Epistemología jurídica y garantismo*. México: Distribuciones Fontamara. Retrieved from http://www.nparangaricutiro.gob.mx/Libros/27.-Epistemologia Juridica Y Garantismo - Ferrajoli, Luigi.pdf

Filmaffinity. (1 983). Juegos de guerra. Retrieved from https://www.filmaffinity.com/es/film553168.html

Fontan Balestra, C. (1 998). *Derecho Penal: Introducción y parte general*. Buenos Aires, Argentina: Abeledo-Perrot.

Foucault, M. (1 998). *Genealogía del racismo*. La Plata, Argentina: Altamira.

Foucault, M. (2 002). *Vigilar y castigar: nacimiento de la prisión*. Buenos Aires, Argentina: Siglo Veintiuno.

Frisancho Aparicio, M. (2 011). *Delitos contra la fe pública*. Lima: Avril Editores.

Frosini, V. (1 983). De la informática jurídica al derecho informático. *Rivista Informatica E Diritto*. Retrieved from http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_02_043-051_Frosini.pdf

Fujimori Fujimori, A. (2 000, May 30). Oficio N° 056-2000-PR. Lima. Retrieved from http://www2.congreso.gob.pe/Sicr/TraDocEstProc/tradoc_condoc_1995.nsf/0/8d4c13d7c161113e05257f2a0059ecc0/$FILE/OBAU0507120000531.pdf

Gabbatt, A. (2 013, August 24). NSA analysts “wilfully violated” surveillance systems, agency admits. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/aug/24/nsa-analysts-abused-surveillance-systems

Gálvez Villegas, Tomás Aladino Delgado Tovar, W. J. (2 011). *Derecho Penal Parte Especial T. II*. Lima: Jurista Editores.

Gercke, M. (2 013). ENFOQUES JURÍDICOS PARA TIPIFICAR EL DELITO DE HURTO DE IDENTIDAD. In *Manual sobre los delitos relacionados con la identidad* (pp. 1–57). Nueva York: Naciones Unidas. Retrieved from https://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf

Gestión. (2 016, December 19). 12 países con el Internet más rápido del mundo. *Gestión*. Lima. Retrieved from https://gestion.pe/tecnologia/12-paises-internet-mas-rapido-mundo-2177435/12

Gestión. (2 016, July 25). Nueva tecnología de Internet móvil LTE Advanced llegó a Perú. *Gestión*. Lima. Retrieved from http://gestion.pe/tecnologia/nueva-tecnologia-internet-movil-lte-advanced-llego-peru-2166314

Gilles, D. (1 999). Post-scriptum sobre las sociedades de control. Valencia: Pre-Textos. Retrieved from http://www.oei.org.ar/edumedia/pdfs/T10_Docu1_Conversaciones_Deleuze.pdf

Glave, J. (1 999). CRACKING THE MIND OF A HACKER. Retrieved from https://www.wired.com/1999/01/cracking-the-mind-of-a-hacker/

Gómez Vieites, A. (2 014). La lucha contra el ciberterrorismo y los ataques informáticos. Retrieved from http://www.edisa.com/wp-content/uploads/2014/08/La_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf

Guarnieri, C., & Schosser, M. (2 013). KeyBoy, Targeted Attacks against Vietnam and India | Rapid7 Community and Blog. Retrieved June 6, 2017, from https://community.rapid7.com/community/infosec/blog/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india

Gutteridge, H. C. (1 946). *Comparative Law*. Londres, Inglatera: Cambridge at The University Press. Retrieved from https://books.google.com.pe/books?id=5nI3AAAAIAAJ

Hall, A. (n.d.). Tipos de delitos informáticos. Retrieved from http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

Henry, K. M. (2 012). *Penetration Testing: Protecting Networks and Systems*. Cambridgeshire, United Kingdom: IT Governance Publishing. Retrieved from https://books.google.com.pe/books?id=CSfJBAAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Heredia Obregón, S. (2 015). POLÍTICA CRIMINAL DE LOS DELITOS INFORMÁTICOS. Retrieved June 3, 2017, from http://www.lozavalos.com.pe/alertainformativa/index.php?mod=contenido&com=contenido&id=19903

HONORABLE CONGRESO DE LA NACION ARGENTINA. (2 008, June 25). MODIFICACION DEL CODIGO PENAL [Ley 26388].

Hulsman, Louk. (1 993). El enfoque abolicionista: Políticas criminales alternativas. Retrieved from https://ia800808.us.archive.org/13/items/Hulsman-1993-ElEnfoqueAbolicionistaPolticasCriminalesAlt.pdf/Hulsman-1993-ElEnfoqueAbolicionistaPolticasCriminalesAlt.pdf

Hurtado Pozo, J. (2 017). DESDE FRIBOURG DERECHO PENAL E INTERNET. Retrieved from http://perso.unifr.ch/derechopenal/assets/files/tribuna/tr_20170408_01.pdf

Hurtado Pozo, J., & Prado Saldarriaga, V. R. (2 011). *Manual de derecho penal: parte general* (4th ed.). Lima: IDEMSA.

Infobae. (2 004, September 13). La primera red informática surgió en la Guerra Fría. Retrieved from http://www.infobae.com/2004/09/13/139362-la-primera-red-informatica-surgio-la-guerra-fria/

Infobae. (2 017, May 12). Ciberataque mundial impacta a instituciones estatales y privadas en una dimensión nunca antes vista. Buenos Aires. Retrieved from

http://www.infobae.com/america/mundo/2017/05/12/ciberataque-mundial-impacta-a-instituciones-estatales-y-privadas-en-una-dimension-nunca-antes-vista/

Insider.pro. (2 016). El espionaje cibernético: la nueva arma de Teherán. Retrieved June 5, 2017, from https://es.insider.pro/opinion/2016-08-11/el-espionaje-cibernetico-la-nueva-arma-de-teheran/

ITU. (2 009). *EL CIBERDELITO: GUÍA PARA LOS PAÍSES EN DESARROLLO*. Ginebra, Suiza: Unión Internacional de Telecomunicaciones. Retrieved from https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

JUAN CARLOS I. Código Penal de España [Ley Orgánica 10/1995] (1995). Retrieved from https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf

Kaspersky. (2 017). Mapa en tiempo real de amenazas cibernéticas Kaspersky. Retrieved from https://cybermap.kaspersky.com/es/

Kaufman, A. (2 013). *Estudios de derecho penal*. Buenos Aires, Argentina: B de F.

Kelly, H. (1977, June 28). Ribicoff offers bill to prevent computer theft. *Chicago Tribune*, p. 36. Chicago. Retrieved from http://archives.chicagotribune.com/1977/06/26/page/36/article/ribicoff-offers-bill-to-prevent-computer-theft

Kindhäuser, U. (2 014). Derecho penal de la seguridad. Los peligros del derecho penal en la sociedad del riesgo. *Revista Pensamiento Penal*, 2027–1743. Retrieved from http://www.pensamientopenal.com.ar/system/files/2014/10/doctrina40016.pdf

Laws.com. (n.d.). Easy Definition of Hacking. Retrieved from http://cyber.laws.com/hacking

Leavitt, D. (2 006). *El hombre que sabía demasiado: Alan Turing y la invención de la computadora*. Barcelona, España: Antoni Bosch Editor. Retrieved from https://books.google.com.pe/books?id=KkQY9fKUpQ4C

Lofgren, M. (2 016). *The Deep State: The Fall of the Constitution and the Rise of a Shadow Government*. New York, USA: Penguin Books. Retrieved from https://books.google.com.pe/books?id=jPoWCAAAQBAJ

López Martinez, H. (2 011). *Historía del Perú: La República contemporánea (1933-2010)*. Lima: El Comercio.

Lyons, J. (2 017, April 3). Guerra cibernética y ciberterrorismo. *El Mundo*. Madrid. Retrieved from http://www.elmundo.es/economia/2017/03/28/58da300a22601d4a3e8b4649.html

MacAskill, E. (2 013, June 10). Edward Snowden, NSA files source: "If they want to get you, in time they will" | US news | The Guardian. Retrieved from https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why

Magro Servet, V. (2 010). Delitos y delincuentes informáticos. In *Delitos y delincuentes* (pp. 109–135). Alicante: Ed. Club Universitario.

Manssen, G. (2 014, June). El "Derecho fundamental a la confidencialidad e integridad de sistemas informáticos"- un aporte exitoso a la creación de derechos de libertad? *Boletin N° 35 Del Instituto de Estudios Constitucionales*, 31–44. Retrieved from http://190.85.246.40/estudios_constitucionales/Boletin35/el-derecho-fundamental-a-la-confidencialidad-e-integridad.pdf

MARCIAL PÉREZ, D. (2 016, December 30). Paraguay, Costa Rica, Uruguay y México: los países de Latinoamérica donde más se usan las redes sociales. *El Pais*. México DF. Retrieved from https://elpais.com/internacional/2016/12/30/actualidad/1483055106_448456.html

Marquez Valencia, A. D. (2 012). LA NECESIDAD DE CONTEMPLAR LOS DELITOS INFORMATICOS EN EL CODIGO PENAL DEL ESTADO DE

MICHOACAN. *Debate Procesal Civil Digital*. Retrieved from http://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/indice.htm

Marquis-Boire, Morgan; Guarnieri, Claudio; Gallagher, R. (2 014, November 24). SECRET MALWARE IN EUROPEAN UNION ATTACK LINKED TO U.S. AND BRITISH INTELLIGENCE. *The Intercept*. Retrieved from https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/

MARTI, O. (1 994, March 2). Francia estrena nuevo Código Penal bajo el espíritu de "los derechos del hombre." *El Pais*. Paris. Retrieved from https://elpais.com/diario/1994/03/02/sociedad/762562801_850215.htmlhttps://elpais.com/diario/1994/03/02/sociedad/762562801_850215.html

Martínez Gutiérrez, R., & Cantó López, M. T. (2 010). *Temario de Derecho Informático (Relaciones Jurídicas Básicas)*. Alicante, España.

Mattelart, A. (2 009). *Un mundo vigilado*. Barcelona, España: Ediciones Paidos Iberica. Retrieved from https://books.google.com.pe/books/about/Un_mundo_vigilado.html?id=PPsrsS4e5LMC

Mattelart, A. (2 002). *Historia de la sociedad de la información*. Barcelona, España: Paidós.

Mayer Lux, L. (2 017). EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS. *Revista Chilena de Derecho*, *44*, 235–260. http://doi.org/http://dx.doi.org/10.4067/S0718-34372017000100011

McLuhan, Marshall; Powers, B. R. (1 993). *La aldea global* (2nd ed.). Barcelona, España: Editorial Gedisa, S.A. Retrieved from

https://monoskop.org/images/2/2c/McLuhan_Marshall_Powells_BR_La_aldea_global.pdf

Mendoza, M. A. (2 016). ¿Fuga, filtración o pérdida de información? Retrieved from https://www.welivesecurity.com/la-es/2016/12/27/fuga-filtracion-perdida-de-informacion/

Migliorisi, D. F. (2 014). La problemática del cibercrimen. In *Informática y delito* (pp. 271–277). C.B.A.: Infojus. Retrieved from http://catedradeluca.com.ar/wp-content/uploads/2015/05/informatica-y-delito.-grupo-argentino-de-la-asociacion-internacional-de-derecho-penal.pdf

Mir Puig, S. (2 003). *Introducción a las bases del derecho penal* (2nd ed.). Buenos Aires, Argentina: B de F.

Molist, M. (2 014, January 11). La "piratería" informática empezó siendo un juego de niños. *El Mundo*. Barcelona. Retrieved from http://www.elmundo.es/tecnologia/2014/01/11/52d0e54d22601d4d0e8b456a.html

Morales Prats, F. (2 010). El derecho penal y el desarrollo de las tecnologías: Los delitos informáticos. In *Efectos de las TICs sobre los Derechos Humanos* (1st ed., pp. 96–103). Barcelona: Institut de Drets Humans de Catalunya (IDHC). Retrieved from https://www.guao.org/sites/default/files/biblioteca/Efectos de las TICs sobre los Derechos Humanos.pdf

Muñoz Conde, F. (1 999). *Teoría general del delito*. Colombia: Temis.S.A.

Naciones Unidas. (2 013). *El uso de internet con fines terroristas*. Nueva York, Estados Unidos: Naciones Unidas. Retrieved from https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

Nakashima, E. (2 016, April 12). FBI paid professional hackers one-time fee to crack San Bernardino iPhone, p. The Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.5ca400557dd0

Navarro Moldes, L. (2 010). Dependencia de las TIC e imposición cultural. In *Efectos de las TICs sobre los Derechos Humanos* (1st ed., pp. 38–56). Barcelona: Institut de Drets Humans de Catalunya (IDHC). Retrieved from https://www.guao.org/sites/default/files/biblioteca/Efectos de las TICs sobre los Derechos Humanos.pdf

Northcutt, S. (n.d.). Logic Bombs, Trojan Horses, and Trap Doors. Retrieved from https://www.sans.edu/cyber-research/security-laboratory/article/log-bmb-trp-door

Norton. (2 017). Malware. Retrieved from https://us.norton.com/internetsecurity-malware.html

Núñez Ponce, J. (1 999). Los delitos informáticos. *Revista Electrónica de Derecho Informático, 15*. Retrieved from https://libros-revistas-derecho.vlex.es/vid/delitos-informaticos-107414

ONU. (1 989). Convención sobre los Derechos del Niño. Retrieved from https://www.unicef.org/argentina/spanish/7.-Convencionsobrelosderechos.pdf

ONU. (2 000). Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía. Retrieved from http://www.ohchr.org/SP/ProfessionalInterest/Pages/OPSCCRC.aspx

Organización Mundial del Comercio. (n.d.). Acuerdo de la Ronda Uruguay: ADPIC Aspectos de los derechos de propiedad intelectual relacionados con el comercio. Retrieved from http://www.wipo.int/treaties/es/text.jsp?file_id=305906

Palacios Rodríguez, R. (2 014). *Historia de la República del Perú [1933-2000]*. (H. López Martinez, Ed.). Lima: Producciones Cantabria S.A.C.

Papa Francisco. (2 017). DISCURSO DEL SANTO PADRE FRANCISCO A LOS PARTICIPANTES EN UN CONGRESO SOBRE "LA DIGNIDAD DEL MENOR EN EL MUNDO DIGITAL." Retrieved from https://w2.vatican.va/content/francesco/es/speeches/2017/october/documents/papa-francesco_20171006_congresso-childdignity-digitalworld.html

Papa Francisco. (2 015). *Laudato Si' : Carta encíclica del Sumo Pontífice Francisco sobre el cuidado de la casa común.* (1st ed.). Lima, Perú: Paulinas. Retrieved from http://w2.vatican.va/content/francesco/es/encyclicals/documents/papa-francesco_20150524_enciclica-laudato-si.pdf

Parker, D. B. (1 989). *COMPUTER CRIME*. Washington, USA: National Institute of Justice. Retrieved from https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf

Parkvall, S., Dahlman, E., Furuskär, A., Jading, Y., Olsson, M., Wänstedt, S., & Zangi, K. (2 009). LTE-Advanced – Evolving LTE towards IMT-Advanced. *Ericsson Research*. Retrieved from https://www.ericsson.com/res/thecompany/docs/journal_conference_papers/wireless_access/VTC08F_jading.pdf

Peña Cabrera Freyre, A. R. (2 015). *Derecho Penal Parte Especial T. II* (2nd ed.). Lima: IDEMSA.

Peña Cabrera Freyre, A. R. (2 015). *Derecho Penal Parte General. T. I* (5th ed.). Lima, Perú: IDEMSA.

Peña Cabrera, R. (1 986). *Tratado de derecho penal V. I* (3rd ed.). Lima, Perú: Sagitario.

Pérez, A. H. (2 002). La prevención de los delitos: elementos fundamentales en la seguridad pública. *Revista de Administración Pública*, *1*(106). Retrieved from https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-administracion-publica/article/view/19140/17242

Pirenne, J. (1 980). *Historia Universal X* (17th ed.). México: Editorial Cumbre, S.A.

Polaino Navarrete, M. (2008). *Introducción al derecho penal* (1st ed.). Lima, Perú: Grijley.

Real Academia Española. (2 014). *Diccionario de la lengua española* (23rd ed.). Madrid, España. Retrieved from http://dle.rae.es

Real Academia Española. (2 003). Diccionario de la lengua española (22 Ed). Madrid: Editorial Espasa Calpe.

Requena Hidalgo, J. (2 004). DE LA SOCIEDAD DISCIPLINARIA A LA SOCIEDAD DE CONTROL: LA INCORPORACIÓN DE NUEVAS TECNOLOGÍAS A LA POLICÍA. *Scripta Nova : Revista Electrónica de Geografía Y Ciencias Sociales*, *8*. Retrieved from http://www.ub.edu/geocrit/sn/sn-170-43.htm

Reyna Alfaro, L. M. (2 002). *Los delitos informáticos: aspectos criminológicos, dogmáticos y de política criminal*. Jurista Editores.

Riquert, M. A. (2 014). Convenio sobre Cibercriminalidad de Budapest y el Mercosur. In *Informática y Delito* (pp. 167–235). Buenos Aires: Infojus.

Rivero, M. (2 016). ¿Qué son los malwares? Retrieved from https://www.infospyware.com/articulos/que-son-los-malwares/

Roca de Estrada, P. (2 001). Delito informático, virus y legislación. *SAIJ*. Retrieved from http://www.saij.gob.ar/doctrina/dacf010038-roca_de_estrada-delito_informatico_virus_legislacion.htm?bsrc=ci

Rogers, M. (n.d.). A New Hacker Taxonomy. Retrieved from http://www.dvara.net/hk/hacker_doc.pdf

Rouse, M. (n.d.). piggybacking. Retrieved from http://whatis.techtarget.com/definition/piggybacking

Roxin, C. (2 014). *Teoría del Tipo Penal*. Buenos Aires, Argentina: B de F.

Roxin, C. (2 002). Problemas actuales de la política criminal. In *Problemas fundamentales de política criminal y derecho penal* (1st ed.). México: Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas.

RT. (2 017, November 9). CIA wrote code “to impersonate” Russia’s Kaspersky Lab anti-virus company, WikiLeaks says. Retrieved from https://www.rt.com/news/409376-cia-wrote-code-to-impersonate-kaspersky/

RT. (2 017, August 24). CIA’s secret spy tool helps agency steal data from NSA & FBI, WikiLeaks reveals. Retrieved from https://www.rt.com/viral/400743-cia-expresslane-data-wikileaks/

RT. (2 017, August 3). Dumbo: WikiLeaks reveals CIA system to take over webcams, microphones. Retrieved from https://www.rt.com/viral/398411-cia-wikileaks-webcam-surveillance/

RT. (2 014, December 22). China se opone a cualquier tipo de ciberataque y ciberterrorismo. *RT*. Retrieved from https://actualidad.rt.com/actualidad/161131-china-oponerse-ciberataques-ciberterrorismo

RT. (2 017, May 12). El Ministerio del Interior de Rusia sufre un ataque cibernético. *RT*. Retrieved from https://actualidad.rt.com/actualidad/238315-ministerio-interior-rusia-sufrir-ataque-cibernetico

RT. (2 017, May 12). Expertos culpan a una "ciberarma" secreta de la NSA del masivo ataque cibernético global - RT. *RT*.Retrieved from https://actualidad.rt.com/actualidad/238324-snowden-responsable-nsa-ataque-cibernetico

RT. (2 017, May 15). ¿Quién es el joven "hacker" amante de la pizza que salvó al mundo del virus WannaCry? - RT. Retrieved from https://actualidad.rt.com/actualidad/238546-marcus-hutchins-hombre-salvo-mundo-virus-wannacry

Rubio Correa, M. (2 009). *El sistema jurídico : introducción al derecho* (10th ed.). Lima: Pontificia Universidad Católica del Perú, Fondo Editorial.

Salinas Siccha, R. (2 008). *Derecho Penal Parte Especial* (3rd ed.). Lima: Iustitia.

Santiago Nino, C. (1 989). *Consideraciones sobre la dogmática jurídica*. UNAM, Instituto de Investigaciones Jurídicas. Retrieved from https://biblio.juridicas.unam.mx/bjv/detalle-libro/892-consideraciones-sobre-la-dogmatica-juridica-con-referencia-particular-a-la-dogmatica-penal-1a-reimp

Sartori, G. (2 004). *Homo videns: la sociedad teledirigida*. Madrid, España: Taurus. Retrieved from http://centromemoria.gov.co/wp-content/uploads/2013/11/Homo_Videns_La_sociedad_teledirigida.pdf

Save The Children. (2 003). *La violencia contra la infancia a través de las tecnologías de la información y la comunicación*. Madrid: Save The Children. Retrieved from http://www.bizkaia.eus/Gizartekintza/Genero_Indarkeria/blt33/documentos/STC_TIC_c.pdf?redirigido=1

Schjolberg, S. (2 008). The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva. Retrieved from http://cybercrimelaw.net/documents/cybercrime_history.pdf

SECUTATIS. (n.d.). PREVENCIÓN DE FUGA DE DATOS. Retrieved from http://www.secutatis.com/?page_id=157

Segu.info. (n.d.). Legislación y Delitos Informáticos - Francia. Retrieved from http://www.segu-info.com.ar/delitos/francia.htm

Senate and House of Representatives of the United States of America in Congress. (1998, October 30). Identity Theft and Assumption Deterrence Act. Retrieved from https://www.ftc.gov/node/119459

Sieber, U. (1 998). *Legal Aspects of Computer-Related Crime in the Information Society*. European Commission. Retrieved from http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf

Sieber, U. (2 015). Risk Society and Preventive Criminal Law [Ponencia en la Universidad Nacional del Altiplano de Puno/Perú]. Puno: Instituto Max Planck para el Derecho penal extranjero e internacional de Friburgo.

Sieber, U. (2 008). Límites del Derecho Penal. Fundamentos y desafíos del nuevo programa de investigación jurídico-penal en el Instituto Max-Planck de Derecho Penal extrajero e internacional. *Revista Penal*. Retrieved from http://www.uhu.es/revistapenal/index.php/penal/article/viewFile/366/357

Silva Santiesteban, F. (1 983). *Historia del Perú T. I.* (3rd ed.). Lima, Perú: Ediciones Buho.

Stallman, R. (2 013). ¿Cuánta vigilancia puede soportar la democracia? *Boletín «Free Software Supporter»*. Retrieved from https://www.gnu.org/philosophy/surveillance-vs-democracy.es.html

Stanger, J., Lane, P. T., & Tim, C. (2 002). *CIW Security Professional Study Guide*. San Francisco, London: SYBEX. Retrieved from https://books.google.com.pe/books?id=GoiecJ9tC2MC&pg=PA172

Sutherland, E. H. (2 009). *El delito de cuello blanco*. Buenos Aires, Argentina: B de F.

Téllez Valdés, J. A. (2 008). *Derecho informático* (4th ed.). México: McGraw-Hill Interamericana.

Tiedemann, K. (1 985). Criminalidad mediante computadoras. *Nuevo Foro Penal*, *30*, 481–492. Retrieved from http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080527_20.pdf

Tompkins Jr, J. B., & Linda A., M. (1 986). THE 1984 FEDERAL COMPUTER CRIME STATUTE: A PARTIAL ANSWER TO A PERVASIVE PROBLEM. *Computer/Law Journal*, *6*(3), 459–483. Retrieved from http://repository.jmls.edu/cgi/viewcontent.cgi?article=1512&context=jitpl

UK Essays. (2 015). The Basics Of Trapdoor Hacking Information Technology Essay. Retrieved from https://www.ukessays.com/essays/information-technology/the-basics-of-trapdoor-hacking-information-technology-essay.php

UNODC. (n.d.). *Mini guía de seguridad informática*. Retrieved from http://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Safety_Guide_Spanish.pdf

UNODC. (2 012). *Compendio de casos de delincuencia organizada*. New York, USA: Naciones Unidas. Retrieved from https://www.unodc.org/documents/organized-crime/SpanishDigest_Final291012.pdf

Vaquero Sanchéz, Antonio; Joyanes Aguilar, L. (1 985). *Informática: Glosario de términos y siglas*. México DF, México.

Viega Rodríguez, M. J. (n.d.). Un nuevo desafío jurídico: Los Delitos Informáticos. Retrieved from http://studylib.es/doc/4610736/delitos-informaticos---maría-josé-viega-rodriguez

Villalón Huerta, A. (2 016). *Amenazas Persistentes Avanzadas*. Valencia, España: Nau Llibres. Retrieved from https://books.google.com.pe/books/about/Amenazas_Persistentes_Avanzadas.html?id=t_ORDQAAQBAJ

Villavicencio Terreros, F. (2 015). DELITOS INFORMÁTICOS EN LA LEY 30096 Y LA MODIFICACIÓN DE LA LEY 30071. *REVISTA VIRTUAL DEL CENTRO DE ESTUDIOS EN DERECHO PENAL*, *2*. Retrieved from http://www.derecho.usmp.edu.pe/cedp/revista/edicion_1/articulos/Felipe_Villavicencio_Terreros-Delitos_Informaticos_Ley30096_su_modificacion.pdf

Washingtonpost.com. (2 003, May 16). Timeline: The U.S. Government and Cybersecurity. Washington. Retrieved from http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html

Welzel, H. (1 956). *Derecho penal: parte general*. Buenos Aires: Depalma.

Westby, J. (2 003). *International Guide to Combating Cybercrime*. Chicago, USA: ABA books. Retrieved from https://books.google.com.pe/books?id=wMqk28WPOf0C

WikiLeaks. (2 017). ExpressLane v3.1.1 -- User Manual. Retrieved from https://wikileaks.org/vault7/document/ExpressLane-3_1_1-User_Manual-Rev_New_2009-04-06/page-1/#pagination

Zaffaroni, E. R. (2 011). *La palabra de los muertos*. Buenos Aires, Argentina: EDIAR.

Zaffaroni, E. R. (2 009a). *Estructura básica del derecho penal*. Buenos Aires, Argentina: Ediar.

Zaffaroni, E. R. (2 009b). *Manual de circunvención o abuso de menores e incapaces*. Buenos Aires, Argentina: Ediar.

Zaffaroni, E. R. (2 012). Apuntes sobre el bien jurídico: fusiones y (con)fusiones, 233–245. Retrieved from http://www.corteidh.or.cr/tablas/usuario/233u.pdf

Zaffaroni, E. R. (1 988). *Criminología : aproximación desde un margen*. Bogotá: Temis. Retrieved from https://colectivociajpp.files.wordpress.com/2012/08/criminologc3ada-aproximacic3b3n-desde-un-margen-zaffaroni.pdf

Zaffaroni, E. R. (1 989). *En busca de las penas perdidas: deslegitimiación y dogmática jurídico-penal*. Ediar.

Zaffaroni, E. R. (1 998). *Tratado de derecho penal: parte general (T. I)*. Buenos Aires: Ediar.

Zaffaroni, E. R. (2 005). *En torno de la cuestión penal*. Buenos Aires: B de F.

Zaffaroni, E. R. (2 015). El derecho latinoamericano en la fase superior del colonialismo. *Passagens. Revista Internacional de História Política E Cultura Jurídica*, *7*(2), 182–243. Retrieved from http://www.redalyc.org/articulo.oa?id=337338776002

Zaffaroni, E. R. (2 014). ¿Derecho penal humano o inhumano? *Revista Pensamiento Penal*, *IV*. Retrieved from http://www.pensamientopenal.com.ar/system/files/2016/05/doctrina43435.pdf

Zaffaroni, E. R. (2 016). *Derecho penal humano y poder en el siglo XXI* (1st ed.). Bogotá, Colombia: Grupo Editorial Ibañez. Retrieved from http://www.pensamientopenal.com.ar/system/files/2016/10/doctrina44188.pdf

Zaffaroni, E. R., Alagia, A., & Slokar, A. (2 011). *Manual de derecho penal, parte general* (2nd ed.). Buenos Aires, Argentina: EDIAR.

Zaffaroni, E. R., Alagia, A., & Slokar, A. (2 002). *Derecho penal: parte general*. Buenos Aires, Aregentina: EDIAR.

Código Orgánico Integral Penal de Ecuador [Código]. (2 014, February 10). Retrieved from http://www.justicia.gob.ec/wp-content/uploads/2014/05/código_orgánico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

CODIGO PENAL DE LA NACION ARGENTINA [LEY 11.179]. (1 984). Retrieved from http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

Code pénal [Código]. (2 017, September 17). Retrieved from https://www.legifrance.gouv.fr/affichCode.do;jsessionid=F1F56C8FFA514BC5371002F65EE15C9E.tplgfr25s_3?cidTexte=LEGITEXT000006070719&dateTexte=20171010

Strafgesetzbuch (StGB) [Código]. (2 017, August 17). Retrieved from https://www.gesetze-im-internet.de/stgb/BJNR001270871.html

U.S. Code [Código]. (2 017, September 1). The Office of the Law Revision Counsel. Retrieved from http://uscode.house.gov/

ANEXOS

ANEXO 1

LEY 30 096

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República

Ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY DE DELITOS INFORMÁTICOS

CAPÍTULO I

FINALIDAD Y OBJETO DE LA LEY

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

CAPÍTULO II

DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

Artículo 2. Acceso ilícito

El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado. (*)

(*) Artículo modificado por el Artículo 1 de la Ley 30 171, publicada el 10 marzo 2 014, cuyo texto es el siguiente:

“Artículo 2. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado."

Artículo 3. Atentado contra la integridad de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa. (*)

(*) Artículo modificado por el Artículo 1 de la Ley 30 171, publicada el 10 marzo 2 014, cuyo texto es el siguiente:

"Artículo 3. Atentado a la integridad de datos informáticos

El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

Artículo 4. Atentado contra la integridad de sistemas informáticos

El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa. (*)

(*) Artículo modificado por el Artículo 1 de la Ley 30 171, publicada el 10 marzo 2 014, cuyo texto es el siguiente:

"Artículo 4. Atentado a la integridad de sistemas informáticos

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

CAPÍTULO III

DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. (*)

(*) Artículo modificado por el Artículo 1 de la Ley 30 171, publicada el 10 marzo 2 014, cuyo texto es el siguiente:

"Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal."

CAPÍTULO IV

DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Artículo 6. Tráfico ilegal de datos

El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. (*)

(*) Artículo derogado por la Única Disposición Complementaria Derogatoria de la Ley 30 171, publicada el 10 marzo 2 014.

Artículo 7. Interceptación de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte

dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales. (*)

(*) Artículo modificado por el Artículo 1 de la Ley 30 171, publicada el 10 marzo 2 014, cuyo texto es el siguiente:

"Artículo 7. Interceptación de datos informáticos

El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27 806, Ley de Transparencia y Acceso a la Información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."

CAPÍTULO V

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 8. Fraude informático

El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social. (*)

(*) Artículo modificado por el Artículo 1 de la Ley 30 171, publicada el 10 marzo 2 014, cuyo texto es el siguiente:

"Artículo 8. Fraude informático

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."

CAPÍTULO VI

DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

Artículo 9. Suplantación de identidad

El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

CAPÍTULO VII

DISPOSICIONES COMUNES

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. (*)

(*) Artículo modificado por el Artículo 1 de la Ley 30 171, publicada el 10 marzo 2 014, cuyo texto es el siguiente:

"Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será

reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.”

Artículo 11. Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.

2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

“Artículo 12. Exención de responsabilidad penal

Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos.” (*)

(*) Artículo incorporado por el Artículo 3 de la Ley 30 171, publicada el 10 marzo 2 014.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Codificación de la pornografía infantil

La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada.

La Policía Nacional del Perú y el Ministerio Público establecen protocolos de coordinación en el plazo de treinta días a fin de cumplir con la disposición establecida en el párrafo anterior.

SEGUNDA. Agente encubierto en delitos informáticos

El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia

de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

TERCERA. Coordinación interinstitucional de la Policía Nacional del Perú con el Ministerio Público

La Policía Nacional del Perú fortalece al órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la Policía Nacional del Perú centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad. (*)

(*) Disposición modificada por el Artículo 2 de la Ley 30 171, publicada el 10 marzo 2 014, cuyo texto es el siguiente:

"TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados

La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, el centro de respuesta temprana del gobierno para ataques cibernéticos (Pe-CERT), la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad."

CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reforzada en el plazo de treinta días desde la vigencia de la presente Ley. (*)

(*) Disposición modificada por el Artículo 2 de la Ley 30 171, publicada el 10 marzo 2 014, cuyo texto es el siguiente:

"CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, el Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados

de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de treinta días desde la vigencia de la presente Ley."

QUINTA. Capacitación

Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal -especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial- en el tratamiento de los delitos previstos en la presente Ley.

SEXTA. Medidas de seguridad

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector público, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

SÉTIMA. Buenas prácticas

El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas.

OCTAVA. Convenios multilaterales

El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos.

NOVENA. Terminología

Para efectos de la presente Ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001:

a. Por sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

b. Por datos informáticos: toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

DÉCIMA. Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP

La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a

las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente. (*)

(*) Disposición modificada por el Artículo 2 de la Ley 30 171, publicada el 10 marzo 2 014, cuyo texto es el siguiente:

"UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece las multas aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957.

Las empresas de telecomunicaciones organizan sus recursos humanos y logísticos a fin de cumplir con la debida diligencia y sin dilación la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa a fin de que el Organismo Supervisor de Inversión Privada en Telecomunicaciones aplique la multa correspondiente."

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Modificación de la Ley 27 697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional

Modifícase el artículo 1 de la Ley 27 697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional,

modificado por el Decreto Legislativo 991 y por Ley 30 077, en los siguientes términos: (*) RECTIFICADO POR FE DE ERRATAS

"Artículo 1. Marco y finalidad

La presente Ley tiene por finalidad desarrollar legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional.

Solo podrá hacerse uso de la facultad prevista en la presente Ley en los siguientes delitos:

1. Secuestro.

2. Trata de personas.

3. Pornografía infantil.

4. Robo agravado.

5. Extorsión.

6. Tráfico ilícito de drogas.

7. Tráfico ilícito de migrantes.

8. Delitos contra la humanidad.

9. Atentados contra la seguridad nacional y traición a la patria.

10. Peculado.

11. Corrupción de funcionarios.

12. Terrorismo.

13. Delitos tributarios y aduaneros.

14. Lavado de activos.

15. Delitos informáticos."

SEGUNDA. Modificación de la Ley 30 077, Ley contra el crimen organizado

Modifícase el numeral 9 del artículo 3 de la Ley 30 077, Ley contra el crimen organizado, en los siguientes términos:

"Artículo 3. Delitos comprendidos

La presente Ley es aplicable a los siguientes delitos:

(...)

9. Delitos informáticos previstos en la ley penal.” (*)

(*) Confrontar con el Artículo 4 del Decreto Legislativo 1 244, publicado el 29 octubre 2 016.

TERCERA. Modificación del Código Procesal Penal

Modifícase el numeral 4 del artículo 230, el numeral 5 del artículo 235 y el literal a) del numeral 1 del artículo 473 del Código Procesal Penal, aprobado por Decreto Legislativo 957 y modificado por Ley 30 077, en los siguientes términos: (*) RECTIFICADO POR FE DE ERRATAS

“Artículo 230. Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación

(...)

4. Los concesionarios de servicios públicos de telecomunicaciones deberán facilitar, en el plazo máximo de treinta días hábiles, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones, así como la información sobre la identidad de los titulares del servicio, los números de registro del cliente, de la línea telefónica y del equipo, del tráfico de llamadas y los números de protocolo de internet, que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las veinticuatro horas de los trescientos sesenta y cinco días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento. Los servidores de las indicadas empresas deberán guardar secreto acerca de las mismas, salvo que se les citare como testigos al procedimiento. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos o software, se encontrarán obligados a mantener la compatibilidad con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. (*)

(*) Confrontar con el Artículo 6 de la Ley 30 171, publicada el 10 marzo 2 014

Artículo 235. Levantamiento del secreto bancario

(...)

5. Las empresas o entidades requeridas con la orden judicial deberán proporcionar, en el plazo máximo de treinta días hábiles, la información correspondiente o las actas y documentos, incluso su original, si así se ordena, y todo otro vínculo al proceso que determine por razón de su actividad, bajo apercibimiento de las responsabilidades

establecidas en la ley. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Artículo 473. Ámbito del proceso y competencia

1. Los delitos que pueden ser objeto de acuerdo, sin perjuicio de los que establezca la Ley, son los siguientes:

a) Asociación ilícita, terrorismo, lavado de activos, delitos informáticos, contra la humanidad;" (*)

(*) Confrontar con el Artículo 2 del Decreto Legislativo 1301, publicado el 30 diciembre 2 016, el mismo que entró en vigencia a nivel nacional a los noventa (90) días contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano.

CUARTA. Modificación de los artículos 162, 183-A y 323 del Código Penal

Modifícanse los artículos 162, 183-A y 323 del Código Penal, aprobado por el Decreto Legislativo 635, en los siguientes términos:

"Artículo 162. Interferencia telefónica

El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales. (*)

(*) Confrontar con el Artículo 4 de la Ley 30 171, publicada el 10 marzo 2 014.

Artículo 183-A. Pornografía infantil

El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.

La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando:

1. El menor tenga menos de catorce años de edad.

2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173 o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de doce ni mayor de quince años. De ser el caso, el agente será inhabilitado conforme a los numerales 1, 2 y 4 del artículo 36.

Artículo 323. Discriminación

El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas.

Si el agente es funcionario o servidor público, la pena será no menor de dos ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.

La misma pena privativa de libertad señalada en el párrafo anterior se impondrá si la discriminación se ha materializado mediante actos de violencia física o mental, o si se realiza a través de las tecnologías de la información o de la comunicación.” (*)

(*) Confrontar con el Artículo 4 de la Ley 30 171, publicada el 10 marzo 2 014.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria

Deróganse el numeral 4 del segundo párrafo del artículo 186 y los artículos 207-A, 207-B, 207-C y 207-D del Código Penal. (*) RECTIFICADO POR FE DE ERRATAS

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los veintisiete días del mes de setiembre de dos mil trece.

FREDY OTÁROLA PEÑARANDA

Presidente del Congreso de la República

MARÍA DEL CARMEN OMONTE DURAND

Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiún días del mes de octubre del año dos mil trece.

OLLANTA HUMALA TASSO

Presidente Constitucional de la República

JUAN F. JIMÉNEZ MAYOR

Presidente del Consejo de Ministros

ANEXO 2

CONSEJO DE EUROPA

Convenio sobre la ciberdelincuencia

Budapest, 23.XI.2001

PREÁMBULO

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio;

Considerando que el objetivo del Consejo de Europa es conseguir una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información;

En la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada, rápida y operativa;

Convencidos de que el presente Convenio resulta necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable;

Conscientes de la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio de Consejo de Europa para la Protección de los Derechos Humanos y de las

Libertades Fundamentales (1 950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho de todos a defender sus opiniones sin interferencia alguna, así como la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad;

Conscientes igualmente del derecho a la protección de los datos personales, tal y como se reconoce, por ejemplo, en el Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento informatizado de datos personales;

Considerando la Convención de las Naciones Unidas sobre los Derechos del Niño (1 989) y el Convenio de la Organización Internacional del Trabajo sobre las peores formas de trabajo de los menores (1 999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio pretende completar dichos Convenios con objeto de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas encaminadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la ciberdelincuencia, incluidas las medidas adoptadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8;

Recordando las recomendaciones del Comité de Ministros n.º R (85) 10 relativa a la aplicación práctica del Convenio europeo de asistencia judicial en materia penal, en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, n.º R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, n.º R (87) 15 relativa a la regulación de la utilización de datos personales por la policía, n.º R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, así como n.º R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece directrices a los legisladores nacionales para la definición de determinados delitos informáticos, y n.º R (95) 13 relativa a las cuestiones de procedimiento penal vinculadas a la tecnología de la información;

Teniendo en cuenta la Resolución n.º 1, adoptada por los Ministros europeos de Justicia en su XXI Conferencia (Praga, 10 y 11 de junio de 1 997), que recomendaba al Comité de Ministros apoyar las actividades relativas a la ciberdelincuencia desarrolladas por el Comité Europeo de Problemas Penales (CDPC) para aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución n.º 3, adoptada en la XXIII Conferencia de Ministros europeos de Justicia (Londres, 8 y 9 de junio de 2 000), que animaba a las Partes negociadoras a proseguir sus esfuerzos para encontrar soluciones que permitan que el mayor número posible de Estados pasen a ser Partes en el Convenio, y reconocía la necesidad de un sistema rápido y eficaz de cooperación

internacional que refleje debidamente las exigencias específicas de la lucha contra la ciberdelincuencia;

Teniendo asimismo en cuenta el Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1 997), para buscar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa,

Han convenido en lo siguiente:

CAPÍTULO I

Terminología

Artículo 1. Definiciones.

A los efectos del presente Convenio:

a) Por «sistema informático» se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;

b) por «datos informáticos» se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

c) por «proveedor de servicios» se entenderá:

i) Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y

ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;

d) por «datos sobre el tráfico» se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

CAPÍTULO II

Medidas que deberán adoptarse a nivel nacional

Sección 1. Derecho penal sustantivo

Título 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2. Acceso ilícito.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Artículo 3. Interceptación ilícita.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4. Interferencia en los datos.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.

Artículo 5. Interferencia en el sistema.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6. Abuso de los dispositivos.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i) Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;

ii) Una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático,

con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y

b) la posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.

Título 2. Delitos informáticos

Artículo 7. Falsificación informática.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8. Fraude informático.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;

b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Título 3. Delitos relacionados con el contenido

Artículo 9. Delitos relacionados con la pornografía infantil.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c) la difusión o transmisión de pornografía infantil por medio de un sistema informático,

d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del anterior apartado 1, por «pornografía infantil» se entenderá todo material pornográfico que contenga la representación visual de:

a) Un menor comportándose de una forma sexualmente explícita;

b) una persona que parezca un menor comportándose de una forma sexualmente explícita;

c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

3. A los efectos del anterior apartado 2, por «menor» se entenderá toda persona menor de dieciocho años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de dieciséis años.

4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

Título 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Artículo 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el

comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo.

Título 5. Otras formas de responsabilidad y de sanciones

Artículo 11. Tentativa y complicidad.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previstos de conformidad con los artículos 2 a 10 del presente Convenio, con la intención de que se cometa ese delito.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier tentativa de comisión de alguno de los delitos previstos de conformidad con los artículos 3 a 5, 7, 8, 9.1.a) y c) del presente Convenio, cuando dicha tentativa sea intencionada.

3. Cualquier Estado podrá reservarse el derecho a no aplicar, en todo o en parte, el apartado 2 del presente artículo.

Artículo 12. Responsabilidad de las personas jurídicas.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas por cualquier persona física, tanto en calidad individual como en su condición de miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, en virtud de:

a) Un poder de representación de la persona jurídica;

b) una autorización para tomar decisiones en nombre de la persona jurídica;

c) una autorización para ejercer funciones de control en la persona jurídica.

2. Además de los casos ya previstos en el apartado 1 del presente artículo, cada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente Convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.

3. Con sujeción a los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Artículo 13. Sanciones y medidas.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos de conformidad con los artículos 2 a 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Cada Parte garantizará la imposición de sanciones o de medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

Sección 2. Derecho procesal

Título 1. Disposiciones comunes

Artículo 14. Ámbito de aplicación de las disposiciones sobre procedimiento.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección para los fines de investigaciones o procedimientos penales específicos.

2. Salvo que se establezca específicamente otra cosa en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el apartado 1 del presente artículo a:

a) Los delitos previstos de conformidad con los artículos 2 a 11 del presente Convenio;

b) otros delitos cometidos por medio de un sistema informático; y

c) la obtención de pruebas electrónicas de un delito.

3. a) Cualquier Parte podrá reservarse el derecho a aplicar las medidas indicadas en el artículo 20 exclusivamente a los delitos o categorías de delitos especificados en la reserva, siempre que el ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que esa Parte aplique las medidas indicadas en el

artículo 21. Las Partes procurarán limitar dichas reservas para permitir la aplicación más amplia posible de la medida indicada en el artículo 20.

b) Cuando, como consecuencia de las limitaciones existentes en su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas indicadas en los artículos 20 y 21 a las comunicaciones transmitidas en el sistema informático de un proveedor de servicios:

i) Utilizado en beneficio de un grupo restringido de usuarios, y

ii) que no utilice las redes públicas de comunicaciones ni esté conectado a otro sistema informático, ya sea público o privado,

dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Cada Parte procurará limitar este tipo de reservas de forma que se permita la aplicación más amplia posible de las medidas indicadas en los artículos 20 y 21.

Artículo 15. Condiciones y salvaguardas.

1. Cada Parte se asegurará de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950), del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966), y de otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando resulte procedente dada la naturaleza del procedimiento o del poder de que se trate, dichas condiciones incluirán, entre otros aspectos, la supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate.

3. Siempre que sea conforme con el interés público y, en particular, con la correcta administración de la justicia, cada Parte examinará la repercusión de los poderes y procedimientos previstos en la presente sección en los derechos, responsabilidades e intereses legítimos de terceros.

Título 2. Conservación rápida de datos informáticos almacenados

Artículo 16. Conservación rápida de datos informáticos almacenados.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan

razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 17. Conservación y revelación parcial rápidas de datos sobre el tráfico.

1. Para garantizar la conservación de los datos sobre el tráfico en aplicación de lo dispuesto en el artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias:

a) Para asegurar la posibilidad de conservar rápidamente dichos datos sobre el tráfico con independencia de que en la transmisión de esa comunicación participaran uno o varios proveedores de servicios, y

b) para garantizar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos sobre el tráfico para que dicha Parte pueda identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 3. Orden de presentación

Artículo 18. Orden de presentación.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a) A una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y

b) a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.

2. Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos 14 y 14.

3. A los efectos del presente artículo, por «datos relativos a los abonados» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:

a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;

c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

Título 4. Registro y confiscación de datos informáticos almacenados

Artículo 19. Registro y confiscación de datos informáticos almacenados.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de una forma similar:

a) A un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y

b) a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos,en su territorio.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de conformidad con lo dispuesto en el apartado 1.a, y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para éste, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso similar al otro sistema.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de una forma similar los datos informáticos a los que se haya tenido acceso en aplicación de lo dispuesto en los apartados 1 ó 2. Estas medidas incluirán las siguientes facultades:

a) Confiscar u obtener de una forma similar un sistema informático o una parte del mismo, o un medio de almacenamiento de datos informáticos;

b) realizar y conservar una copia de dichos datos informáticos;

c) preservar la integridad de los datos informáticos almacenados de que se trate;

d) hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.

4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los apartados 1 y 2.

5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 5. Obtención en tiempo real de datos informáticos

Artículo 20. Obtención en tiempo real de datos sobre el tráfico.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a:

a) Obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, y

b) obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:

i) a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabaren tiempo real los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21. Interceptación de datos sobre el contenido.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno:

a) A obtener o a grabar mediante la aplicación de medios técnicos existentes en su territorio, y

b) a obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:

i) A obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o

ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar

en tiempo real los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático.

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Sección 3. Jurisdicción

Artículo 22. Jurisdicción.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido:

a) En su territorio; o

b) a bordo de un buque que enarbole pabellón de dicha Parte; o

c) a bordo de una aeronave matriculada según las leyes de dicha Parte; o

d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

2. Cualquier Estado podrá reservarse el derecho a no aplicar o a aplicar únicamente en determinados casos o condiciones las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier otra parte de los mismos.

3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del artículo 24 del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5. Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales.

CAPÍTULO III

Cooperación internacional

Sección 1. Principios generales

Título 1. Principios generales relativos a la cooperación internacional

Artículo 23. Principios generales relativos a la cooperación internacional.

Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

Título 2. Principios relativos a la extradición

Artículo 24. Extradición.

1. a) El presente artículo se aplicará a la extradición entre las Partes por los delitos establecidos en los artículos 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave.

b) Cuando deba aplicarse una pena mínima diferente en virtud de un acuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o

más Partes, incluido el Convenio Europeo de Extradición (STE n.º 24), se aplicará la pena mínima establecida en virtud de dicho acuerdo o tratado.

2. Se considerará que los delitos mencionados en el apartado 1 del presente artículo están incluidos entre los delitos que dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes. Las Partes se comprometen a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí.

3. Cuando una Parte que condicione la extradición a la existencia de un tratado reciba una solicitud de extradición de otra Parte con la que no haya celebrado ningún tratado de extradición, podrá aplicar el presente Convenio como fundamento jurídico de la extradición respecto de cualquier delito mencionado en el apartado 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el apartado 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5. La extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Cuando se deniegue la extradición por un delito mencionado en el apartado 1 del presente artículo únicamente por razón de la nacionalidad de la persona buscada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes para los fines de las actuaciones penales pertinentes, e informará a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomarán su decisión y efectuarán sus investigaciones y procedimientos de la misma manera que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7. a) Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado.

b) El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

Título 3. Principios generales relativos a la asistencia mutua

Artículo 25. Principios generales relativos a la asistencia mutua.

1. Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.

2. Cada Parte adoptará también las medidas legislativas y de otro tipo que resulten necesarias para cumplir las obligaciones establecidas en los artículos 27 a 35.

3. En casos de urgencia, cada Parte podrá transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación, incluidos el fax y el correo electrónico, en la medida en que dichos medios ofrezcan niveles adecuados de seguridad y autenticación (incluido el cifrado, en caso necesario), con confirmación oficial posterior si la Parte requerida lo exige. La Parte requerida aceptará la solicitud y dará respuesta a la misma por cualquiera de estos medios rápidos de comunicación.

4. Salvo que se establezca específicamente otra cosa en los artículos del presente capítulo, la asistencia mutua estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegar la cooperación. La Parte requerida no ejercerá el derecho a denegar la asistencia mutua en relación con los delitos mencionados en los artículos 2 a 11 únicamente porque la solicitud se refiere a un delito que considera de naturaleza fiscal.

5. Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente,.

Artículo 26. Información espontánea.

1. Dentro de los límites de su derecho interno, y sin petición previa, una Parte podrá comunicar a otra Parte información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el presente Convenio o podría dar lugar a una petición de cooperación de dicha Parte en virtud del presente capítulo.

2. Antes de comunicar dicha información, la Parte que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. Si la Parte receptora no puede atender esa solicitud, informará de ello a la otra Parte, que deberá entonces determinar si a pesar de ello debe facilitarse la información o no. Si la Parte destinataria acepta la información en las condiciones establecidas, quedará vinculada por las mismas.

Titulo 4. Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Artículo 27. Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

1. Cuando entre las Partes requirente y requerida no se encuentre vigente un tratado de asistencia mutua o un acuerdo basado en legislación uniforme o recíproca, serán de aplicación las disposiciones de los apartados 2 a 10 del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2. a) Cada Parte designará una o varias autoridades centrales encargadas de enviar solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución y de su remisión a las autoridades competentes para su ejecución.

b) Las autoridades centrales se comunicarán directamente entre sí.

c) En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en cumplimiento del presente apartado.

d) El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con los procedimientos especificados por la Parte requirente, salvo que sean incompatibles con la legislación de la Parte requerida.

4. Además de las condiciones o de los motivos de denegación contemplados en el apartado 4 del artículo 25, la Parte requerida podrá denegar la asistencia si:

a) La solicitud se refiere a un delito que la Parte requerida considera delito político o delito vinculado a un delito político;

b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

5. La Parte requerida podrá posponer su actuación en respuesta a una solicitud cuando dicha actuación pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por sus autoridades.

6. Antes de denegar o posponer la asistencia, la Parte requerida estudiará, previa consulta cuando proceda con la Parte requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que considere necesarias.

7. La Parte requerida informará sin demora a la Parte requirente del resultado de la ejecución de una solicitud de asistencia. Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada. La Parte requerida informará también a la Parte requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.

8. La Parte requirente podrá solicitar a la Parte requerida que preserve la confidencialidad de la presentación de una solicitud en virtud del presente capítulo y del objeto de la misma, salvo en la medida necesaria para su ejecución. Si la Parte requerida no puede cumplir esta petición de confidencialidad, lo comunicará inmediatamente a la Parte requirente, que determinará entonces si pese a ello debe procederse a la ejecución de la solicitud.

9. a) En casos de urgencia, las solicitudes de asistencia mutua o las comunicaciones al respecto podrán ser enviadas directamente por las autoridades judiciales de la Parte requirente a las autoridades correspondientes de la Parte requerida. En tal caso, se enviará al mismo tiempo copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

b) Cualquier solicitud o comunicación en virtud de este apartado podrá efectuarse a través de la Organización Internacional de Policía Criminal (INTERPOL).

c) Cuando se presente una solicitud en aplicación de la letra a) del presente artículo y la autoridad no sea competente para tramitarla, remitirá la solicitud a la autoridad nacional competente e informará directamente a la Parte requirente de dicha remisión.

d) Las solicitudes y comunicaciones efectuadas en virtud del presente apartado que no impliquen medidas coercitivas podrán ser remitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.

e) En el momento de la firma o el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deberán dirigirse a su autoridad central.

Artículo 28. Confidencialidad y restricción de la utilización.

1. En ausencia de un tratado de asistencia mutua o de un acuerdo basado en legislación uniforme o recíproca que esté vigente entre las Partes requirente y requerida, serán de aplicación las disposiciones del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2. La Parte requerida podrá supeditar la entrega de información o material en respuesta a una solicitud a la condición de que:

a) Se preserve su confidencialidad cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de esta condición, o

b) no se utilicen para investigaciones o procedimientos distintos de los indicados en la solicitud.

3. Si la Parte requirente no puede cumplir alguna condición de las mencionadas en el apartado 2, informará de ello sin demora a la otra Parte, que determinará en tal caso si

pese a ello debe facilitarse la información. Cuando la Parte requirente acepte la condición, quedará vinculada por ella.

4. Cualquier Parte que facilite información o material con sujeción a una condición con arreglo a lo dispuesto en el apartado 2 podrá requerir a la otra Parte que explique, en relación con dicha condición, el uso dado a dicha información o material.

Sección 2. Disposiciones especiales

Título 1. Asistencia mutua en materia de medidas provisionales

Artículo 29. Conservación rápida de datos informáticos almacenados.

1. Una Parte podrá solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.

2. En las solicitudes de conservación que se formulen en virtud del apartado 1 se indicará:

a) La autoridad que solicita dicha conservación;

b) el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;

c) los datos informáticos almacenados que deben conservarse y su relación con el delito;

d) cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;

e) la necesidad de la conservación; y

f) que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

3. Tras recibir la solicitud de otra Parte, la Parte requerida tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble tipificación penal como condición para proceder a la conservación.

4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para

creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.

5. Asimismo, las solicitudes de conservación únicamente podrán denegarse si:

a) La solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;

b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

6. Cuando la Parte requerida considere que la conservación por sí sola no bastará para garantizar la futura disponibilidad de los datos o pondrá en peligro la confidencialidad de la investigación de la Parte requirente o causará cualquier otro perjuicio a la misma, informará de ello sin demora a la Parte requirente, la cual decidirá entonces si debe pese a ello procederse a la ejecución de la solicitud.

7. Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el apartado 1 tendrán una duración mínima de sesenta días, con objeto de permitir a la Parte requirente presentar una solicitud de registro o de acceso de forma similar, confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma.

Artículo 30. Revelación rápida de datos conservados sobre el tráfico.

1. Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo 29 para la conservación de datos sobre el tráfico en relación con una comunicación específica, la Parte requerida descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.

2. La revelación de datos sobre el tráfico en virtud del apartado 1 únicamente podrá denegarse si:

a) La solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;

b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Título 2. Asistencia mutua en relación con los poderes de investigación

Artículo 31. Asistencia mutua en relación con el acceso a datos informáticos almacenados.

1. Una Parte podrá solicitar a otra Parte que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un

sistema informático situado en el territorio de la Parte requerida, incluidos los datos conservados en aplicación del artículo 29.

2. La Parte requerida dará respuesta a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con otras disposiciones aplicables en el presente capítulo.

3. Se dará respuesta lo antes posible a la solicitud cuando:

a) Existan motivos para creer que los datos pertinentes están especialmente expuestos al riesgo de pérdida o modificación; o

b. los instrumentos, acuerdos o legislación mencionados en el apartado 2 prevean la cooperación rápida.

Artículo 32. Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público.

Una Parte podrá, sin la autorización de otra Parte:

a) Tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos; o

b) tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.

Artículo 33. Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico.

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en su territorio transmitidas por medio de un sistema informático. Con sujeción a lo dispuesto en el apartado 2, dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno.

2. Cada Parte prestará dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país.

Artículo 34. Asistencia mutua relativa a la interceptación de datos sobre el contenido.

Las Partes se prestarán asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que lo permitan sus tratados y el derecho interno aplicables.

Título 3. Red 24/7

Artículo 35. Red 24/7.

1. Cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:

a) El asesoramiento técnico;

b) la conservación de datos en aplicación de los artículos 29 y 30;

c) la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

2. a) El punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente.

b) Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.

3. Cada Parte garantizará la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red.

CAPÍTULO IV

Disposiciones finales

Artículo 36. Firma y entrada en vigor.

1. El presente Convenio estará abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales tres como mínimo sean Estados miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

4. Respecto de cualquier Estado signatario que exprese más adelante su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado

su consentimiento para quedar vinculado por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

Artículo 37. Adhesión al Convenio.

1. Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros.

2. Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

Artículo 38. Aplicación territorial.

1. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Estado podrá especificar el territorio o territorios a los que se aplicará el presente Convenio.

2. En cualquier momento posterior, mediante declaración dirigida al Secretario General del Consejo de Europa, cualquier Parte podrá hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. Respecto de dicho territorio, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.

3. Toda declaración formulada en virtud de los dos apartados anteriores podrá retirarse, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido dicha notificación.

Artículo 39. Efectos del Convenio.

1. La finalidad del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones de:

– El Convenio europeo de extradición, abierto a la firma en París el 13 de diciembre de 1957 (STE n.º 24);

– el Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 20 de abril de 1959 (STE n.º 30);

– el Protocolo adicional al Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 17 de marzo de 1978 (STE n.º 99).

2. Si dos o más Partes han celebrado ya un acuerdo o tratado sobre las materias reguladas en el presente Convenio o han regulado de otra forma sus relaciones al respecto, o si lo hacen en el futuro, tendrán derecho a aplicar, en lugar del presente Convenio, dicho acuerdo o tratado o a regular dichas relaciones en consonancia. No obstante, cuando las Partes regulen sus relaciones respecto de las materias contempladas en el presente Convenio de forma distinta a la establecida en el mismo, deberán hacerlo de una forma que no sea incompatible con los objetivos y principios del Convenio.

3. Nada de lo dispuesto en el presente Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de las Partes.

Artículo 40. Declaraciones.

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir elementos complementarios según lo dispuesto en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e).

Artículo 41. Cláusula federal.

1. Los Estados federales podrán reservarse el derecho a asumir las obligaciones derivadas del capítulo II del presente Convenio de forma compatible con los principios fundamentales por los que se rija la relación entre su gobierno central y los estados que lo formen u otras entidades territoriales análogas, siempre que siga estando en condiciones de cooperar de conformidad con el capítulo III.

2. Cuando formule una reserva en aplicación del apartado 1, un Estado federal no podrá aplicar los términos de dicha reserva para excluir o reducir sustancialmente sus obligaciones en relación con las medidas contempladas en el capítulo II. En todo caso, deberá dotarse de una capacidad amplia y efectiva que permita la aplicación de las medidas previstas en dicho capítulo.

3. Por lo que respecta a las disposiciones del presente Convenio cuya aplicación sea competencia de los estados federados o de otras entidades territoriales análogas que no estén obligados por el sistema constitucional de la federación a la adopción de medidas legislativas, el gobierno federal informará de esas disposiciones a las autoridades competentes de dichos estados, junto con su opinión favorable, alentándoles a adoptar las medidas adecuadas para su aplicación.

Artículo 42. Reservas.

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el apartado 2 del artículo 4, apartado 3 del artículo 6, apartado 4 del artículo 9, apartado 3 del artículo 10, apartado 3 del artículo 11, apartado 3 del artículo 14, apartado 2 del artículo 22, apartado 4 del artículo 29 y apartado 1 del artículo 41. No podrán formularse otras reservas.

Artículo 43. Situación de las reservas y retirada de las mismas.

1. La Parte que haya formulado una reserva de conformidad con el artículo 42 podrá retirarla en todo o en parte mediante notificación dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica que la retirada de una reserva surtirá efecto en una fecha especificada en la misma y ésta es posterior a la fecha en que el Secretario General reciba la notificación, la retirada surtirá efecto en dicha fecha posterior.

2. La Parte que haya formulado una reserva según lo dispuesto en el artículo 42 retirará dicha reserva, en todo o en parte, tan pronto como lo permitan las circunstancias.

3. El Secretario General del Consejo de Europa podrá preguntar periódicamente a las Partes que hayan formulado una o varias reservas según lo dispuesto en el artículo 42 acerca de las perspectivas de que se retire dicha reserva.

Artículo 44. Enmiendas.

1. Cualquier Estado Parte podrá proponer enmiendas al presente Convenio, que serán comunicadas por el Secretario General del Consejo de Europa a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio, así como a cualquier Estado que se haya adherido al presente Convenio o que haya sido invitado a adherirse al mismo de conformidad con lo dispuesto en el artículo 37.

2. Las enmiendas propuestas por una Parte serán comunicadas al Comité Europeo de Problemas Penales (CDPC), que presentará al Comité de Ministros su opinión sobre la enmienda propuesta.

3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados Partes no miembros en el presente Convenio, podrá adoptar la enmienda.

4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con el apartado 3 del presente artículo será remitido a las Partes para su aceptación.

5. Cualquier enmienda adoptada de conformidad con el apartado 3 del presente artículo entrará en vigor treinta días después de que las Partes hayan comunicado su aceptación de la misma al Secretario General.

Artículo 45. Solución de controversias.

1. Se mantendrá informado al Comité Europeo de Problemas Penales del Consejo de Europa (CDPC) acerca de la interpretación y aplicación del presente Convenio.

2. En caso de controversia entre las Partes sobre la interpretación o aplicación del presente Convenio, éstas intentarán resolver la controversia mediante negociaciones o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia

al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes o a la Corte Internacional de Justicia, según acuerden las Partes interesadas.

Artículo 46. Consultas entre las Partes.

1. Las Partes se consultarán periódicamente, según sea necesario, con objeto de facilitar:

a) La utilización y la aplicación efectivas del presente Convenio, incluida la detección de cualquier problema derivado del mismo, así como los efectos de cualquier declaración o reserva formulada de conformidad con el presente Convenio;

b) el intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico;

c) el estudio de la conveniencia de ampliar o enmendar el presente Convenio.

2. Se mantendrá periódicamente informado al Comité Europeo de Problemas Penales (CDPC) acerca del resultado de las consultas mencionadas en el apartado 1.

3. Cuando proceda, el CDPC facilitará las consultas mencionadas en el apartado 1 y tomará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Como máximo tres años después de la entrada en vigor del presente Convenio, el Comité Europeo de Problemas Penales (CDPC) llevará a cabo, en cooperación con las Partes, una revisión de todas las disposiciones del Convenio y, en caso necesario, recomendará las enmiendas procedentes.

4. Salvo en los casos en que sean asumidos por el Consejo de Europa, los gastos realizados para aplicar lo dispuesto en el apartado 1 serán sufragados por las Partes en la forma que éstas determinen.

5. Las Partes contarán con la asistencia de la Secretaría del Consejo de Europa para desempeñar sus funciones en aplicación del presente artículo.

Artículo 47. Denuncia.

1. Cualquier Parte podrá denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 48. Notificación.

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido al mismo o que haya sido invitado a hacerlo:

a) Cualquier firma;

b) el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;

c) cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;

d) cualquier declaración formulada en virtud del artículo 40 o reserva formulada de conformidad con el artículo 42;

e) cualquier otro acto, notificación o comunicación relativo al presente Convenio.

En fe de lo cual, los infrascritos, debidamente autorizados a tal fin, firman el presente Convenio.

Hecho en Budapest, el 23 de noviembre de 2001, en francés e inglés, siendo ambos textos igualmente auténticos, en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copias certificadas a cada uno de los Estados Miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado invitado a adherirse al mismo.